TUGAS AKHIR – TE 141599

# Pengembangan *Identity Federation* pada *Test Bed* IdREN (*Indonesia Research Education Network*)

Ary Budi Prakoso
NRP 22150105060

Dosen Pembimbing
Dr. Ir. Achmad Affandi, DEA
Ir. Djoko Suprajitno Rahardjo, MT.

DEPARTEMEN TEKNIK ELEKTRO
Fakultas Teknologi Elektro
Institut Teknologi Sepuluh Nopember
Surabaya 2017


*FINAL PROJECT* – TE 141599

# *Developing Identity Federation at IDREN Test Bed*

Ary Budi Prakoso
NRP 22151051060

*Supervisor*
Dr. Ir. Achmad Affandi, DEA
Ir. Djoko Suprajitno Rahardjo, MT.

*ELECTRICAL ENGINEERING DEPARTMENT*
*Faculty of Electrical Technology*
Institut Teknologi Sepuluh Nopember
Surabaya 2017

# PERNYATAAN KEASLIAN
# TUGAS AKHIR

Dengan ini saya menyatakan bahwa isi sebagian maupun keseluruhan Tugas Akhir saya dengan judul "**Pengembangan *Identity Federation* pada *Test Bed* IdREN (*Indonesia Research Education Network*)**" adalah benar-benar hasil karya intelektual mandiri, diselesaikan tanpa menggunakan bahan-bahan yang tidak diijinkan dan bukan merupakan karya pihak lain yang saya akui sebagai karya sendiri.

Semua referensi yang dikutip maupun dirujuk telah ditulis secara lengkap pada daftar pustaka.

Apabila ternyata pernyataan ini tidak benar, saya bersedia menerima sanksi sesuai peraturan yang berlaku.

Surabaya, 5 Juni 2017

Ary Budi Prakoso
NRP. 2215105060

*Halaman ini sengaja dikosongkan*

# PENGEMBANGAN *IDENTITY FEDERATION* PADA *TEST BED* IDREN (*INDONESIA RESEARCH EDUCATION NETWORK*)

## TUGAS AKHIR

**Diajukan Guna Memenuhi Sebagian Persyaratan**
**Untuk Memperoleh Gelar Sarjana Teknik**
**Pada**
**Bidang Studi Telekomunikasi Multimedia**
**Departemen Teknik Elektro**
**Fakultas Teknologi Elektro**
**Institut Teknologi Sepuluh Nopember**

**Menyetujui:**

| Dosen Pembimbing I, | Dosen Pembimbing II, |
|---|---|
| **Dr. Ir. Achmad Affandi, DEA** | **Ir. Djoko Suprajitno Rahardjo, MT.** |
| **NIP. 196510141990021001** | **NIP. 195506221987011000** |

**SURABAYA**
**JULI 2017**

**Pengembangan *Identity Federation* pada *Test Bed* IdREN (*Indonesia Research Education Network*)**

**Nama** : Ary Budi Prakoso
**Pembimbing** : Dr. Ir. Achmad Affandi, DEA
Ir. Djoko Suprajitno Rahardjo, MT.

# ABSTRAK

Di tahun 2002 kawasan Eropa menjadi basis terselenggaranya interkoneksi antara dunia pendidikan dan lembaga penelitian. Inter koneksi tersebut bernama eduroam (*education roaming*). Eduroam adalah layanan *roaming* internasional untuk pengguna dalam penelitian, pendidikan tinggi dan pendidikan lanjutan. Di Indonesia ada dua perguruan tinggi yang sudah terhubung dengan eduroam, ITB dan yang baru saja bergabung adalah UII. Sedangkan di Indonesia eduroam bernama IDREN (*Indonesia Research Education Network*). IdREN dulu dikenal dengan Inherent (*Indonesia Higher Education Network*).

Pada bulan september 2015 jaringan IdREN sudah menghubungkan lima *gate*/*router* IdREN yang terdapat di 5 perguruan tinggi. Jaringan tersebut dihubungkan dengan *gateway* TEIN melalui ITB, sehingga sudah bisa mengakses REN dari negara lain dan juga internet2. Dengan terbentuknya jaringan IdREN, diharapkan dapat memudahkan mahasiswa untuk mengakses internet di perguruan tinggi lain yang sudah terhubung dengan IdREN. Mahasiswa cukup memasukkan akun email mereka di hotspot perguruan tinggi lain.

Tugas akhir ini membahas miniatur/simulasi tentang struktur jaringan IdREN yang dapat menghubungkan lima perguruan tinggi. Sehingga judul tugas akhir menggunakan kata *test bed* yang berarti miniatur/simulasi. Setiap perguruan tinggi diasumsikan sebuah *router* yang dapat terhubung dengan *router* lainnya. *Routing protocol* yang digunakan dalam *test bed* jaringan IdREN yaitu BGP dan OSPF. Terdapat mekanisme *Identity Federation* dalam *test bed* jaringan IdREN. Sharing database digunakan untuk mempermudah komunikasi antar perguruan tinggi yaitu dengan LDAP (*Light Weight Directory Access Protocol*). Sistem keamanan menggunakan SSL (*Security Socket Layer*) dengan membangun *self signed certificate*.

**Kata Kunci** – *Test Bed* Jaringan IDREN, LDAP, SSL

*Halaman ini sengaja dikosongkan*

***Developing Identity Federation at IDREN Test Bed***

***Name*** **:** Ary Budi Prakoso
***Supervisor*** **:** Dr. Ir. Achmad Affandi, DEA
Ir. Djoko Suprajitno Rahardjo, MT.

# *ABSTRACT*

*In 2002 the European region became the basis for interconnection between education and research institutions. Inter connection is called eduroam (education roaming). Eduroam is an international roaming service for users in research, higher education and further education. In Indonesia there are two universities that have been connected with eduroam, ITB and who just joined is UII. While in Indonesia eduroam named IDREN (Indonesia Research Education Network). IdrEN was once known as Inherent (Indonesia Higher Education Network).*

*In September 2015 IdREN network has connected five gate / router IdREN contained in 5 colleges. The network is connected to the TEIN gateway via ITB, so that it can access REN from other countries and also internet2. With the establishment of IdREN network, is expected to facilitate students to access the internet at other universities that are connected with IdREN. Students simply enter their email account at other college hotspots.*

*This final project discusses miniatur / simulation about the network structure of IdREN that can connect five universities. So the title of the final task using the word test bed which means miniature / simulation. Each college assumed a router that can connect with other routers. Routing protocols used in the IdREN network test bed are BGP and OSPF. There is an Identity Federation mechanism in the IdREN network test bed. Sharing database is used to facilitate communication between universities that is with LDAP (Light Weight Directory Access Protocol). The security system uses SSL (Security Socket Layer) by building self signed certificate.*

***Keywords*** *– IdREN tes bed, LDAP, SSL*

.

*Halaman ini sengaja dikosongkan*

# KATA PENGANTAR

Segala puji syukur penulis panjatkan atas kehadirat Allah SWT yang selalu memberikan rahmat serta hidayah-Nya sehingga Tugas Akhir ini dapat terselesaikan dengan baik. Shalawat serta salam selalu dilimpahkan kepada Nabi Muhammad SAW, keluarga, sahabat, dan umat muslim yang senantiasa meneladani beliau.

Pada kesempatan ini penulis ingin mengucapkan ucapan terimakasih yang sebesar-besarnya kepada beberapa pihak yang telah memberikan dukungan selama proses pengerjaan tugas akhir ini, antara lain:

1. Keluarga penulis Bapak Agus Rahardjo, Kakak Teguh, Ibu Sri Budiati, dan seluruh keluarga yang selalu memberikan doa, motivasi, semangat, perhatian dan kasih sayangnya.
2. Bapak Dr. Ir. Achmad Affandi, DEA dan Bapak Ir. Djoko Suprajitno Rahardjo, MT., selaku dosen pembimbing serta selalu memberikan arahan dan ilmu dalam penyelesaian Tugas Akhir ini.
3. Seluruh dosen program studi Telekomunikasi Departemen Teknik Elektro FTE ITS.
4. Dan seluruh teman-teman LJ Teknik Elektro, serta banyak pihak yang tidak dapat disebutkan satu-persatu atas kebersamaannya.

Penulis menyadari bahwa dalam Tugas Akhir ini terdapat banyak kekurangan. Akhir kata semoga melalui tulisan ini dapat bermanfaat dan dapat berbagi ilmu bagi pembacanya. Amin.

Surabaya, 5 Juni 2017

Penulis

*Halaman ini sengaja dikosongkan*

# DAFTAR ISI

# TABLE OF CONTENT

# DAFTAR GAMBAR

# DAFTAR TABEL

*Halaman ini sengaja dikosongkan*

# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

Di tahun 2002 kawasan Eropa menjadi basis terselenggaranya interkoneksi antara dunia pendidikan dan lembaga penelitian. Inter koneksi tersebut bernama eduroam (*education roaming*). Eduroam adalah layanan roaming internasional untuk pengguna dalam penelitian, pendidikan tinggi dan pendidikan lanjutan. Baru tahun 2004 eduroam masuk ke wilayah Amerika tepatnya di Kanada. Eduroam sudah menyebar ke berbagai belahan dunia, tak terkecuali di daerah Asia-Pasifik. Di Indonesia ada dua perguruan tinggi yang sudah terhubung dengan eduroam, ITB dan yang baru saja bergabung adalah UII. Sedangkan di Indonesia eduroam bernama IDREN (Indonesia *Research Education Network*). IdREN dulu dikenal dengan Inherent (Indonesia Higher Education Network. Yang terbaru jaringan IDREN menggunakan *gateway* TEIN melalui ITB dengan internet2 sudah menghubungkan 5 perguruan tinggi di Indonesia (ITB, UI, ITS, UB, UGM).

Pada bulan september 2015 jaringan IdREN sudah menghubungkan lima *gate*/*router* IdREN yang terdapat di 5 perguruan tinggi. Jaringan tersebut dihubungkan dengan *gateway* TEIN melalui ITB, sehingga sudah bisa mengakses REN dari negara lain dan juga internet 2. Dengan terbentuknya jaringan IdREN, diharapkan dapat memudahkan mahasiswa untuk mengakses internet di perguruan tinggi lain yang sudah terhubung dengan IdREN. Mahasiswa cukup memasukkan akun email mereka di hotspot perguruan tinggi lain.

Tugas akhir ini membahas miniatur/simulasi tentang struktur jaringan IdREN yang dapat menghubungkan lima perguruan tinggi. Sehingga judul tugas akhir menggunakan kata *test bed* yang berarti miniatur/simulasi. Setiap perguruan tinggi diasumsikan sebuah *router* yang dapat terhubung dengan *router* lainnya. Terdapat mekanisme *Identity Federation* dalam jaringan IdREN. *Identity federation* adalah sebuah kebijakan atau aturan untuk mengatur satu identitas antara pengguna dan perangkat pada jaringan yang berbeda. Satu akun dapat digunakan di jaringan kampus lain yang telah terhubung jaringan IdREN. Terdapat *sharing database* untuk mempermudah komunikasi antar perguruan tinggi. LDAP (*Light Weight Directory Access Protocol*)

adalah sebuah protokol yang mendefinisikan bagaimana data disimpan secara terpusat dan dapat diakses melalui jaringan. Diperlukan kemanan untuk menjaga kerahasiaan akun setiap mahasiswa di dalam jaringan IdREN. Sistem keamanan menggunakan SSL (*Security Socket Layer*) dengan membangun *self signed certificate*.

### 1.2. Rumusan Masalah

1. Bagaimana membuat test bed jaringan IdREN?
2. Bagaimana merancang *sharing authority access* di test bed jaringan IdREN?
3. Bagaimana merancang *security policy* pada *test bed* jaringan IDREN?

### 1.3. Batasan Masalah

Berdasarkan permasalahan yang telah diuraikan di atas, batasan masalah dari tugas akhir ini adalah:

1. Tugas Akhir ini dibuat hanya sebagai *test bed* tanpa diimplementasi pada jaringan sebenarnya.

### 1.4. Tujuan

Tujuan kami menuliskan tugas akhir ini adalah:

1. Membuat *test bed* jaringan IDREN supaya mengetahui gambaran umum jaringan yang sebenarnya
2. Merancang *sharing autority access* dengan LDAP sebagai direktori untuk menyimpan username dan sandi setiap akun.
3. Merancang *security policy* pada *test bed* jaringan IDREN untuk melindungi data-data pengguna

### 1.5. Metodologi

Dalam pelaksanaan tugas akhir yang berupa pengembangan *identity federation* pada IDREN, ada beberapa kegiatan yang dapat diuraikan sebagai berikut:

a. Studi Literatur
   Pada tahapan ini akan mempelajari beberapa referensi dari jurnal yang berhubungan dengan *identity federation*, *routing* protokol BGP, serta LDAP.
b. Pembuatan *Software* dan *Hardware*
   Untuk simulasi menggunakan *cisco packet tracer student*. Ketika bahan yang dibutuhkan telah terkumpul maka sistem

akan dirangkai secara bertahap untuk menjadi sebuah *test bed* IDREN

c. Uji Coba dan Analisis Data
   Setelah semua sudah dirancang dalam bentuk jadi maka selanjutnya melakukan uji coba, dengan cara meneliti setiap sistem bagian yang telah dirancang. Jika terdapat kesalahan fungsi selanjutnya mencari solusi untuk mengatasi permasalahan tersebut, dengan mengecek kembali alat yang telah dirangkai dan mencocokan data-data yang sudah terkumpul sebelumnya.

## 1.6. Sistematika Laporan

Pembahasan pada laporan Tugas Akhir ini terdiri dari lima bab, yaitu pendahuluan, teori penunjang, perencanaan dan pembuatan alat, pengujian dan analisa alat, serta penutup.

BAB I PENDAHULUAN

Menguraikan latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat yang berkaitan dengan pengerjaan dan penyusunan Tugas Akhir ini.

BAB II TEORI PENUNJANG

Pada bab ini dikemukakan berbagai macam dasar teori yang berhubungan dengan permasalahan yang dibahas, antara lain meliputi teori tentang BGP, IDREN, keamanan jaringan.

BAB III PERENCANAAN DAN PEMBUATAN ALAT

Membahas perencanaan dan pembuatan perangkat keras yang meliputi diagram blok sistem.

BAB IV PENGUJIAN DAN ANALISA SISTEM

Membahas pengujian dan analisa data terhadap penggunaan satu akun pada jaringan IDREN

BAB V PENUTUP

Berisi penutup yang menjelaskan tentang kesimpulan dari tugas akhir ini dan saran-saran untuk pengembangan robot ini lebih lanjut.

## 1.7. Relevansi

Pengembangan *identity federation* pada *test bed* IDREN diharapkan mampu diimplementasikan pada jaringan IDREN yang sebenarnya.

*Halaman ini sengaja dikosongkan*

# BAB II
# TEORI PENUNJANG

## 2.1 Internet2

Kehidupan dunia sekarang ini sangat bergantung pada jaringan-jaringan data yang tersebar secara terpadu maupun secara terpisah, hal ini memungkinkan siapa saja terkoneksi secara suara dan data. Industri telekomunikasi informasi sekarang terus-menerus menghasilkan gelombang baru produk dan jasa telekomunikasi yang dirancang untuk memudahkan memperluas kehidupan manusia, setidaknya itu yang mereka katakan, dan secara bersamaan adalah merebut pasar yang memang terus-menerus menuntut tersedianya produk-produk baru yang lebih baik.

Teknologi internet yang kita kenal sekarang ini bukannya tidak ada permasalahan. Salah satunya adalah tersumbatnya jaringan menjadi bottleneck dalam sistem jaringan yang sekarang ada. Terlalu banyak pengguna koneksi *dial-up*, dan menjadi tidak mungkin dilakukan *streaming* aplikasi multimedia. Selain itu, alamat-alamat internet yang disebut IP *address* (Internet *Protocol*) juga semakin menipis, sehingga perlu perluasan yang masif untuk menopang stabilitas sistem jaringan data dan telekomunikasi yang sekarang terkonvergensi satu sama lain. Kemampuan teknologi baru yang dibutuhkan adalah Internet2.

### 2.1.1 Sejarah Internet2

Keterbatasan internet membuat para ahli komputer untuk berusaha mengembangkan internet lagi supaya lebih baik yang akan mendukung performa tinggi aplikasi seperti data mining, pencitraan medis dan fisika partikel. Hal ini menghasilkan penciptaan yang mempunyai kinerja sangat tinggi Layanan Jaringan Backbone atau vBNS yang dikembangkan pada tahun 1995 oleh *National Science Foundation* (NSF) dan MCI, pengembangan ini khusus untuk memenuhi kebutuhan di lembaga pendidikan superkomputer. Konsep dari "generasi internet" dilahirkan. Dan sebagai hasilnya Internet2 didirikan untuk melayani kebutuhan jaringan. Proyek pendirian internet2 ini awalnya didirikan oleh 34 universitas dan para peneliti pada tahun 1996 di bawah naungan EDUCAUSE dan secara resmi diorganisir sebagai *not-for-profit University Corporation for Advanced Internet Development* (UCAID) pada tahun 1997, kemudian mengubah namanya menjadi Internet2.

Internet2 adalah merek dagang terdaftar. kantor pusat administratif konsorsium Internet2 terletak di Ann Arbor, Michigan, dengan kantor di Washington DC. Komunitas pengguna internet2 mengadakan kerjasama dengan Qwest, membangun Jaringan Internet2 pertama, yang disebut Abilene, pada tahun 1998 menjadi proyek utama dari investor perusahaan LambdaRail Nasional (NLR). Selama 2004-2006, Internet2 dan NLR mengadakan diskusi mengenai penggabungan kedua perusahaan itu. Tapi pembicaraan Mereka berhenti karena perbedaan yang belum terpecahkan. Pada tahun 2006, Internet2 mengumumkan kemitraan dengan Level 3 Communications untuk meluncurkan jaringan nasional baru, dengan meningkatkan kapasitasnya dari 10 Gbps menjadi 100 Gbps. Pada bulan Oktober 2007, Internet2 Abilene resmi mengacu pada kapasitas jaringan yang lebih besar sebagai Internet2 Network.

### 2.1.2 Tujuan Internet2

Internet2 menyediakan informasi-informasi bagi penelitian di AS dan komunitas pendidikan dengan jaringan yang membutuhkan *bandwidth* secara intensif. Jaringan itu sendiri bersifat dinamis, cepat, kuat, dan hemat biaya. Ini melengkapi untuk 100GB/s kekuatan jaringan lebih dari 210 lembaga-lembaga pendidikan Amerika Serikat, 70 perusahaan, 45 non-profit dan lembaga pemerintah. Namun, bukan hanya versi yang lebih cepat dari internet sekarang ini, tapi juga berfungsi sebagai akses teknologi jaringan baru, teknologi kolaborasi baru, dan teknologi instruksional baru. Sebagai contoh, Internet2 akan digunakan untuk prototipe baru

1. QOS (kualitas-of-service) kontrol sehingga memungkinkan untuk memberikan perlakuan khusus untuk aplikasi yang mengkonsumsi sejumlah besar data atau gambar, sedangkan transmisi teks lebih lambat.
2. *Multicast* teknik sehingga memungkinkan untuk mendistribusikan pesan secara efisien untuk 100-atau 1000s situs. Saat ini membutuhkan 100-atau 1000s transmisi.
3. Jaringan berbasis video *conference* membuat berkualitas tinggi, *desktop* ke *desktop* interaksi mungkin tanpa harus membeli atau menyewa jalur komunikasi khusus

Lebih lanjut, Internet2 dirancang untuk mempercepat pengembangan teknologi baru untuk komunitas pendidikan nasional dan untuk umum (komersial) jaringan, sehingga

semua jaringan menjadi lebih fleksibel dan lebih efisien. Internet2 akan berperan dalam menentukan jaringan masa depan akan seperti apa, dan bagaimana masa depan pendidikan berbasis jaringan nanti.

### 2.1.3 Definisi Internet2

Internet2 adalah konsorsium jaringan canggih terkemuka AS. Didirikan oleh para peneliti dan lembaga pendidikan sejak tahun 1996, Internet2 mempromosikan misi dari para anggotanya dengan menyediakan terdepan baik kemampuan jaringan kemitraan yang unik dan kesempatan yang bersama-sama memfasilitasi pengembangan, penyebaran dan penggunaan teknologi internet revolusioner. Jaringan Internet2 yang maju, jaringan performa tinggi yang mendukung aplikasi maju atau kompleks yang tidak bekerja di Internet komersial atau tidak bekerja dengan baik. Jaringan Internet2 menyediakan konektivitas antara lembaga dan konektivitas riset internasional dan jaringan pendidikan sehingga memberikan akses ke riset global dan pendidikan masyarakat.

### 2.1.4 Keunggulan Internet2

Jaringan Internet2 yang berkinerja tinggi berpengaruh di seluruh dunia dan mengadakan kemitraan untuk mendukung dan meningkatkan pendidikan dan penelitian misi. Lebih dari sekedar menyediakan kapasitas jaringan, Internet2 aktif melibatkan komunitas kita dalam pengembangan teknologi baru yang penting termasuk middleware, keamanan, jaringan riset dan pengukuran kinerja kemampuan yang sangat penting untuk kemajuan Internet.

Internet2 menyediakan penelitian dan pendidikan AS komunitas dengan dinamis, inovatif dan hemat biaya hibrida paket optik dan jaringan. Jaringan ini dirancang untuk memberikan generasi mendatang layanan produksi serta platform untuk pengembangan ide-ide baru dan protokol jaringan. Dengan kontrol komunitas jaringan fundamental infrastruktur, Jaringan Internet2 memberikan skalabilitas yang diperlukan bagi lembaga anggota yang efisien untuk penyediaan sumber daya untuk mengatasi kebutuhan *bandwidth*-intensif kampus mereka seperti, kolaborasi aplikasi, didistribusikan penelitian eksperimen, grid berbasis analisis data dan jaringan sosial.

Para peneliti California Institute of Technology (Caltech) di Pasadena, Amerika Serikat dan CERN yang berpusat di Geneva, Swiss telah menguji kecepatan transfer data pada jaringan backbone Internet2,

Abilene Network. Penelitian dilakukan untuk mengukur kecepatan pengiriman data sejauh 11.000 kilometer dengan kecepatan rata-rata 6,25 gigabits per second (gbps)

Menurut pernyataan CERN yang dikutip IDG News Service, kecepatan transfer yang didapatkan ternyata 10.000 kali kecepatan koneksi internet broadband rumahan. "Riset menujukkan *high energy physics*, astrofisika, energi fusi, klimatologi, bioinformatika, dan bidang lainnya memerlukan jaringan internet yang cepat," tutur Harvey Newman, profesor Fisika di Universitas Caltech, Amerika Serikat. "Dalam jangka 10 tahun mendatang kecepatan transfer data akan mencapai *terabit per second* (1 trilyun bits)."

Dengan internet2,sebuah kendaraan yang dioperasikan jarak jauh membuat jalan di bawah air sebagai bagian dari ekspedisi Ballard untuk menjelajahi bidang *vent* hidrotermal pada pertengahan Samudera Atlantik. Dari dalam sebuah laboratorium di University of Washington, Professor Deborah Kelley bisa mengemudikan pesawat, seolah-olah ia sedang bermain video game di Internet2. "Kita tidak bisa melakukan ini dengan komoditi internet, karena *latency*."Dengan Internet2, tidak ada *latency*, tidak ada penundaan, tidak perlu menunggu kendaraan untuk bereaksi atau *overcompensate*.

Sekarang ini, Internet2 masih belum tersedia untuk umum. Karena tujuan utama Internet2 adalah untuk menciptakan kemampuan jaringan unggulan bagi riset dan pengembangan, melakukan percobaan-percobaan atas produk *router* dan serat optik yang baru, dan menciptakan jasa jaringan dan aplikasi yang baru bagi standar internet. Di masa depan, penggunaan jaringan internet akan melibat kelompok manusia dalam jumlah yang sangat besar. Dan ini belum termasuk proyek-proyek yang merupakan konvergensi telekomunikasi, hiburan digital, perangkat perumahan, industri komputer dan lainnya.

## 2.2 Eduroam

Eduroam (*Education Roaming*) adalah layanan *roaming* internasional untuk pengguna dalam penelitian, pendidikan tinggi dan pendidikan lanjut. Hal ini memberi peneliti, dosen dan siswa mengakses jaringan yang mudah dan aman saat mengunjungi institusi lain. Autentikasi dilakukan oleh institusi asal mereka, menggunakan kredensial yang sama seperti saat mereka mengakses jaringan secara lokal, sementara autorisasi untuk mengakses internet dan kemungkinan sumber daya lainnya ditangani oleh institusi yang dikunjungi. Dan hal

lainnya adalah pengguna tidak harus membayar untuk menggunakan eduroam.

## 2.3 REN (*Research Education Network*)

REN adalah sebuah jaringan yang tujuan penggunaannya dalam bidang riset dan pendidikan. Dari segi infrastruktur sendiri saja REN di Indonesia masih kalah jauh dengan negara Thailand. Di negara Thailand, setiap universitas di kota terhubung dengan koneksi REN yang memiliki *bandwidth* sekitar 1-10 Gbps. Sedangkan di Indonesia? koneksi REN antar universitas dengan *bandwidth* 1Gbps pun masih susah, bahkan bisa di kata belum ada. Koneksi dengan beberapa universitas ada yang masih menggunakan *bandwidth* relatif kecil 1Mbps, 2 Mbps itupun kadang juga bukan jalur REN tetapi melalui jalur internet. Kenapa seperti itu? Karena, mungkin menurut saya salah satu alasannya, pembangunan di Indonesia belumlah merata. Sehingga, medium untuk mengkoneksikan universitas-universitas tersebut bermacam-macam, ada yang menggunakan kabel *fiber optic* (dengan kemampuan yang berbeda-beda), adapula yang baru bisa menggunakan teknologi satelit sebagai mediumnya. Ya, tak dapat dipungkiri bahwa memang biaya yang dibutuhkan untuk menyediakan infrastruktur dengan kemampuan seperti yang dimiliki, contohnya, Thailand bukan lah sesuatu yang ringan dan murah.

Tapi, dilihat dari keuntungan yang dapat dirasakan dengan adanya REN tersebut sebanding dengan biaya yang dikeluarkan. Dengan adanya *bandwidth* selebar itu, komunikasi jarak jauh dapat dilakukan dengan leluasa yang berakibat dapat dilakukannya kelas/kuliah jarak jauh tanpa adanya gangguan kualitas dikarenakan kurangnya *bandwidth* yang berimbas pada kualitas gambar dan suara dari kegiatan kuliah jarak jauh tersebut. Acara-acara kegiatan yang melibatkan antar universitas di Indonesia dapat diselenggarakan dengan mudah. Rapat pejabat antar universitas atau dengan pihak-pihak lain dapat cukup dilaksanakan di daerah masing-masing tanpa harus bertemu di suatu tempat tertentu dengan menggunakan teknologi video *conference*, hal ini dapat menghemat pengeluaran biaya, waktu, dan waktu untuk transportasi ke daerah lain. Kerjasama riset komputasi paralel melalui jaringan dengan grid atau cloud mungkin juga dapat dilakukan karena lebarnya *bandwidth* yang ada.

Palapa Ring adalah suatu proyek pembangunan jaringan serat optik nasional yang akan menjangkau sebanyak 33 provinsi, 440

kota/kabupaten di seluruh Indonesia dengan total panjang kabel laut mencapai 35.280 kilometer, dan kabel di daratan adalah sejauh 21.807 kilometer. Namun, sayangnya proyek ini masih belum selesai juga walaupun sudah cukup lama proyek ini diusulkan. Dengan adanya proyek ini, ada kemungkinan dapat menekan biaya internet di Indonesia, memperlebar *bandwidth* koneksi lokal di Indonesia, mendorong penyediaan konten lokal Indonesia, ataupun dapat digunakan sebagai koneksi REN di Indonesia. Dan proyek ini ditargetkan akan selesai pada tahun 2013.

Dengan adanya palapa *ring* ini dapat memajukan teknologi yang ada di Indonesia ini, sehingga kita tidak kalah bersaing dalam bidang teknologi setidaknya dengan negara-negara tetangga kita sendiri. Walau sebenarnya Indonesia sendiri sudah memiliki 2 REN, yaitu Jardiknas dan INHERENT. INHERENT ini merupakan REN di tingkat universitas, sedangkan Jardiknas pada tingkat di bawahnya. Untuk konektivitas dengan REN luar negeri Indonesia terkoneksi melalui TEIN 3 yang terkoneksi pada INHERENT dan ITB. Sebelum TEIN 3, Indonesia terkoneksi REN dengan TEIN 2 dan AIII Jepang yang terkoneksi pada jaringan ITB. Saat ini pihak ITB sendiri masih bekerja sama dengan pihak AIII Jepang dalam pelaksanaan beberapa kuliah jarak jauh.

## 2.4 TEIN

TEIN4 merupakan generasi keempat dari TEIN (*Trans-Eurasia Information Network*), yang menyediakan jaringan penelitian dalam skala besar dan komunikasi data pendidikan untuk regional Asia-Pasifik. Tujuan dari TEIN4 adalah untuk memperluas konektivitas penelitian dan pendidikan, menghubungkan peneliti, pengajar dan pelajar yang berada dalam regional Asia-Pasifik serta civitas pendidikan di seluruh dunia. TEIN4 bekerja sama dengan DANTE, APAN, TransPAC3, *Pacific Wave*, dan Internet2.

ITB terhubung dalam TEIN sejak generasi kedua pada tahun 2004, yang kemudian menjadi TEIN3 pada tahun 2008. Dengan bergabungnya ITB dengan TEIN2, ITB menjadi gerbang untuk menghubungkan INHERENT (*Indonesia Higher Education Network*) dengan TEIN3 sehingga universitas-universitas di Indonesia dapat terhubung dengan universitas-universitas yang berada di Asia-Pasifik dan Eropa. Diagram jaringan TEIN3 dapat dilihat pada gambar berikut. Perubahan yang terjadi dalam TEIN4 untuk ITB adalah peningkatan kapasitas *bandwidth*

menjadi 622 Mbps dengan koneksi langsung ke Singapura dimana sebelumnya kapasitas *bandwidth* yang ada sebesar 155 Mbps dan koneksi ke Hongkong.

Melalui proyek TEIN 2, Uni Eropa akan mengalokasikan dana untuk membantu agar ITB mampu mendapatkan *bandwidth* 45 Mbps. Tepatnya, biaya yang harus dikeluarkan untuk mendapatkan *bandwidth* ekstra 45 Mbps adalah 150,000 Euro per tahun. Lama proyek TEIN 2 adalah 2 tahun. ITB sendiri tetap berkontribusi sekitar 20 persen dari dana yang harus dikeluarkan. Jalur Routing Pendek Selain keuntungan berupa jalur internet yang sangat "lebar", infrastruktur dalam proyek TEIN 2 memungkinkan proses routing yang lebih pendek. Tentunya ini akan semakin menghemat *bandwidth*. Dengan jalur konvensional, *bandwidth* sebesar 2 Mbps bisa termakan hanya untuk proses routing. Untuk sampai ke jaringan di Jepang, RRC, dan Korea Selatan dari Indonesia, melalui jalur TEIN 2, hanya perlu melewati sebuah *router* di Singapura. Bahkan, Jalur langsung ke jaringan di Uni Eropa pun hanya melewati *router* di Singapura ini.

Dalam kerangka persiapan TEIN 2, telah dipasang kabel fiber optic di ITB Galian tanah dengan kabel-kabel kuning yang mewarnai kampus beberapa bulan lalu adalah proyek pemasangan *fiber optic* di seluruh jaringan ITB oleh PT Indosat, partner SingTel di Indonesia yang memenangkan tender infrastruktur ITB-Singapura. Memanfaatkan TEIN: Membuka Mata "Yang menjadi masalah adalah bagaimana memanfaatkan *bandwidth* sebesar itu," tutur Basuki Suhardiman, pakar jaringan di ITB Untuk itu, ITB sendiri telah mengajak departemen dan kelompok penelitian internal ITB untuk memanfaatkan 45 Mbps ini demi keperluan riset dan pendidikan. Departemen di ITB dapat memanfaatkan jalur ini untuk menyelenggarakan kuliah *teleconference* via internet. "Teleconference itu hanya butuh 2 Mbps, itu sudah menghasilkan gambar yang baik, layaknya berbicara langsung," ungkap Basuki "Departemen Astronomi sudah menyatakan minat untuk bergabung dengan Australia dalam pemantauan bintang di daerah belahan bumi bagian selatan, dalam proyek NASA." Basuki juga mencontohkan, Departemen Geofisika dan Meteorologi dapat juga memanfaatkan ini untuk mendapatkan data *real time* dari NOAA.

Selain itu, ITB juga telah menawarkan perguruan tinggi lain di Indonesia untuk memanfaatkan jaringan ini. Ini merupakan tanggung jawab ITB sebagai wakil Indonesia dalam proyek TEIN 2: membangun jaringan riset dan pendidikan di Indonesia. Sampai sekarang, Universitas

Syiah Kuala dan Universitas Padjadjaran telah menyatakan minatnya turut memanfaatkan *bandwidth* ini. Yang perlu disayangkan dari Proyek TEIN 2 ini, biaya pembangunan *bandwidth* di Indonesia masih terlampau mahal sehingga membengkakkan pengeluaran. Tambahan lagi, di sisi lain, ITB, sendirian, harus tetap membiayai 20 persen dari proyek ini, atau sekitar 60,000 Euro selama dua tahun. Sebagai pembanding, negara jiran, Malaysia, Filipina, dan Thailand membangun *bandwidth* sampai 155 Mbps; sementara Australia, 622 Mbps.

Melalui program TEIN yang akan efektif pada bulan Desember 2005 sampai Desember 2007 ini, diharapkan riset dan dunia pendidikan di Indonesia -bukan hanya di ITB berkembang. Proses pembelajaran Indonesia melalui riset-riset di luar negri, serta pengenalan terhadap riset-riset unggulan Indonesia akan semakin pesat. TEIN 2 bukan hanya sekedar ekstra *bandwidth* yang masif demi download yang cepat. Lebih dari itu, proyek ini akan sekaligus melebarkan wawasan akademisi dan peneliti Indonesia, serta membuka mata dunia untuk 'melirik' Indonesia. Dan ITB akan menjadi lokomotifnya. Saat ini, koneksi TEIN3 digunakan untuk:

- *Video-conference* yang dilakukan oleh ITB dengan universitas-universitas lain yang berada di luar negeri.
- Mengambil data-data meteorologi dari *National Oceanic and Atmospheric Administration* (NOAA) untuk keperluan penelitian yang berhubungan dengan cuaca.
- Menyediakan *repository* FreeBSD dan Linux yang bersifat umum dan dapat digunakan oleh siapapun.

Seluruh civitas akademika ITB dapat memanfaatkan jaringan TEIN4 untuk melakukan kolaborasi penelitian dengan perguruan tinggi lain yang terhubung dengan TEIN4 maupun perguruan tinggi yang berada di Benua Eropa dan Amerika. Untuk dapat memanfaatkan jaringan TEIN4, civitas akademika ITB dapat menghubungi noc@itb.ac.id.

Selain civitas akademika ITB, jaringan TEIN4 juga akan diintegrasikan dengan INHERENT (*Indonesia Higher Education Network*) sehingga semua perguruan tinggi yang tergabung dalam INHERENT juga dapat memanfaatkan jalur TEIN4

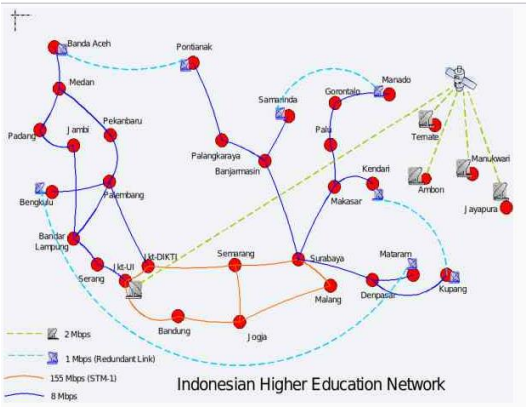
## 2.5 Inherent (*Indonesia Higher Education Network*)

INHERENT merupakan inisiatif dari Direktorat Jenderal Pendidikan Tinggi (Dikti) Departemen Pendidikan Nasional Indonesia untuk membuat sebuah jaringan backbone yang menyambungkan 32

perguruan tinggi negeri yang ada di masing-masing propinsi di seluruh Indonesia.

Desain jaringan INHERENT ini dikemukakan kepada DIKTI atas rumusan rancangan bersama dari Institut Teknologi Bandung (ITB), Universitas Indonesia (UI), Universitas Gajah Mada (UGM) dan Institut Teknologi Surabaya (ITS). Setelah dilaksanakan tender, maka terpilih PT Telkom sebagai penyedia infrastruktur jaringan, serta PT Multipolar sebagai Partner dari Cisco *System* yang menyediakan perangkat jaringan.

Jaringan ini terdiri dari *backbone fiber optic* STM-1 berkecepatan 155 Mbps untuk interkoneksi antara universitas di pulau Jawa, serta backbone *leased channel* berkecepatan 8 Mbps untuk universitas di pulau Sumatera, Kalimantan, Sulawesi serta Bali dan Nusa Tenggara. Universitas di daerah Indonesia Timur mendapatkan akses satelit dari Jakarta dengan kecepatan 2 Mbps. Diagram jaringan dapat dilihat pada gambar 2.1 berikut:




**Gambar 2.1** Jaringan Inherent

Masing-masing universitas negeri yang menjadi tempat POP (*Point of Presence*) dari backbone INHERENT memiliki peralatan *router* dan server dari Cisco *System* dan *Sun Microsystem*. Gambar dari *rack* yang berisi *router* dan server yang terpasang pada POP INHERENT di ITB dapat dilihat pada gambar 2.2 berikut:

**Gambar 2.2** *Router* dan Server di ITB

Jaringan ini telah dinyatakan operasional pada bulan September 2006, dan mendekati 6 bulan operasinya, jaringan ini telah dimanfaatkan oleh berbagai perguruan tinggi untuk mengadakan berbagai aktivitas, misalnya :

1. Video *Conference* Seminar Teknologi *Grid* Computing yang diselenggarakan oleh Sun Microsystem bekerjasama dengan Universitas Indonesia, disaksikan oleh empat universitas (ITB, Unibraw, UNDIP dan UGM).
2. Aktivitas *Web Proxy Cache Peering* antara ITB dengan UI, Unila Lampung dan Unsri Palembang.
3. Aktivitas Video *Conference* untuk rapat antara Dikti dengan Universitas penerima Hibah K-1.

## 2.6 Perangkat Keras Jaringan Komputer

Perangkat keras jaringan komputer adalah perangkat yang digunakan untuk mengubungkan dua atau lebih komputer dalam jaringan komputer agar setiap komputer yang terhubung dapat saling berbagi data, file, dan sumber daya lainnya. Seperti halnya komputer, sebuah jaringan komputer bisa beroperasi dengan didukung oleh software dan hardware. Berikut ini perangkat jaringan komputer :

### 2.6.1 *Network Interface Card* (NIC)

Kartu jaringan atau NIC (*Network Interface Card*) adalah sebuah kartu yang berfungsi sebagai jembatan dari komputer ke sebuah jaringan komputer. Biasa disebut juga sebagai *network adapter*. Setiap NIC memiliki alamat yang disebut MAC *address*, yang dapat bersifat statis tetapi dapat diubah oleh pengguna.

### 2.6.2 *Repeater*

*Repeater* adalah sebuah peralatan jaringan yang berfungsi menangkap sinyal dan mentransmisikan kembali sinyal tersebut dengan kekuatan yang lebih tinggi sehingga sinyal tersebut dapat menempuh jarak yang lebih jauh. Dengan adanya *repeater*, jarak antara beberapa jaringan komputer dapat diperluas.

### 2.6.3 *Hub*

*Hub* adalah *central connection point* pada suatu jaringan. *Hub* tidak memiliki fasilitas *routing*, sehingga semua data yang datang akan di*broadcast* ke semua perangkat yang terhubung padanya. Ada 2 macam *hub*, yaitu *active hub* dan *passive hub*. *Active hub* bertindak juga sebagai *repeater* sedangkan *passive hub* hanya berfungsi untuk mentransmisikan sinyal ke jaringan.

### 2.6.4 *Bridge*

*Bridge* adalah sebuah komponen jaringan yang digunakan untuk memperluas jaringan atau membuat sebuah segmen jaringan. *Bridge* beroperasi di dalam lapisan data-link pada model OSI. *Bridge* juga dapat digunakan untuk menggabungkan dua buah arsitektur jaringan yang berbeda, misalnya antara *Token Ring* dan *Ethernet*. *Bridge* tidak melakukan konversi terhadap protokol, sehingga agar dua segmen jaringan yang dikoneksikan ke *bridge* tersebut dapat terkoneksi, kedua jaringan tersebut harus memiliki protokol jaringan yang sama (misalnya TCP/IP).

### 2.6.5 *Router*

*Router* berfungsi untuk menghubungkan *network* yang satu dengan yang lain dan memilih jalur yang terbaik (*routing*) untuk mengirimkan paket data yang datang dari satu *port* ke *port* yang dituju paket data tersebut. *Router* mengirimkan paket data berdasarkan *IP address*. *Router* adalah sebuah alat (*dedicated*) atau berupa aplikasi yang berfungsi untuk memutuskan pada titik manakah paket data harus diteruskan. *Router* pada umumnya terletak pada *gateway* suatu jaringan. Pada dasarnya cara kerja *router* hampir sama dengan *bridge*, namun *router* tidak mampu mempelajari alamat seperti halnya *bridge*. Akan tetapi *router*, seperti yang sudah disebutkan di atas, dapat menentukan *path* data antar dua jaringan. *Router* dapat mengubungkan dua jaringan

berbeda dengan *subnet* yang berbeda. *Router* memiliki apa yang dinamakan *routing tabel*, yaitu sebuah daftar dari rute yang tersedia dan mampu memilih rute terbaik untuk sebuah paket data.

Secara umum, *router* dibagi menjadi dua jenis, yaitu :

1. *Static router* : adalah *router* yang memiliki tabel *routing* statis yang diset secara manual oleh para administrator jaringan.
2. *Dynamic router* : adalah *router* yang mengatur tabel *routing* secara dinamis. *Router* dinamis menggunakan *routing protocol*, yang secara otomatis menyesuaikan bila ada perubahan topologi dan lalu lintas pada jaringan.

**Gambar 2.3** *Router* Cisco 2800

### 2.6.6 *Switch*

*Switch* adalah suatu perangkat atau *device* yang berfungsi sebagai pengatur dan pembagi sinyal data dari suatu komputer ke komputer lainnya yang terhubung pada perangkat tersebut, fungsi tersebut sama dengan fungsi *hub* yang menjadi perbedaan adalah *switch* bisa melakukan pengaturan berupa proses filter paket data. Biasanya masing-masing *port* pada *switch* bisa diatur sehingga bisa ditentukan *port* mana saja yang bisa saling terhubung. *Switch* beroperasi pada *layer* dua (*datalink layer*) dari OSI model.

**Gambar 2.4** *Switch Cisco* 2960

## *2.7 Subnetting*

*Subnetting* adalah proses membagi atau memecah sebuah *network* menjadi beberapa *network* yang lebih kecil atau yang sering disebut *subnet*. Biasanya penulisan *IP address* dituliskan seperti contoh : 192.168.1.1, tetapi terkadang dituliskan 192.168.1.1/24. Maksud dari penulisan 192.168.1.1/24, berarti IP address 192.168.1.1 dengan *subnet mask* 255.255.255.0 (1111111.11111111.11111111.00000000) atau 24

*bit subnet mask* diisi dengan angka 1. Konsep ini disebut dengan CIDR (*Classless Inter-Domain Routing*) yang diperkenalkan pertama kali tahun 1992 oleh IEFT.

**Tabel 2.1** Nilai CIDR di Masing-masing *Subnet*

| Subnet Mask | Nilai CIDR |
|---|---|
| 255.128.0.0 | /9 |
| 255.192.0.0 | /10 |
| 255.224.0.0 | /11 |
| 255.240.0.0 | /12 |
| 255.248.0.0 | /13 |
| 255.252.0.0 | /14 |
| 255.254.0.0 | /15 |
| 255.255.0.0 | /16 |
| 255.255.128.0 | /17 |
| 255.255.192.0 | /18 |
| 255.255.224.0 | /19 |

| Subnet Mask | Nilai CIDR |
|---|---|
| 255.255.240.0 | /20 |
| 255.255.248.0 | /21 |
| 255.255.252.0 | /22 |
| 255.255.254.0 | /23 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |

## 2.8 Jaringan (*Network*)

Jaringan (*network*) adalah kumpulan dua atau lebih komputer yang masing-masing berdiri sendiri dan terhubung melalui sebuah teknologi. Hubungan antar komputer tersebut tidak terbatas berupa kabel tembaga saja, namun juga bisa melalui *fiber optic*, *microwave*, *infrared*, bahkan melalui satelit.

Tujuan dari penggunaan jaringan komputer adalah :

1. Membagi sumber daya : contoh berbagi pemakaian *printer*, CPU, memori dan *harddisk*.
2. Komunikasi : contohnya surat elektronik, *instant messaging*, dan *chatting*.
3. Akses informasi : contohnya *web browsing*.

Secara umum jaringan mempunyai beberapa manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Adapun manfaat yang didapat dalam membangun suatu jaringan adalah sebagai berikut :

1. *Sharing resources*.
2. Media komunikasi.
3. Integrasi data.
4. Pengembangan dan pemeliharaan.

5. Keamanan data.
6. Sumber daya lebih efisien dan informasi terkini.

### 2.8.1 Klasifikasi Jaringan Komputer

Jaringan komputer atau disingkat jarkom mempunyai klasifikasi atau pengelompokan jaringan tertentu, seperti klasifikasi berdasarkan topologi jaringan, klasifikasi berdasarkan jangkauan geografis, klasifikasi berdasarkan media transmisi, klasifikasi berdasarkan fungsi dan klasifikasi berdasarkan distribusi sumber informasi/data. Dalam kesempatan ini akan membahas klasifikasi berdasarkan jangkauan geografis.

**1. PAN (*Personal Area Network*)**

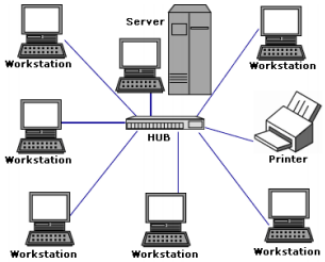
PAN (*Personal Area Network*) adalah jaringan komputer yang digunakan untuk komunikasi antara peralatan komputer dengan *user*. Jangkauan dari PAN biasanya hanya beberapa meter saja (6-9 meter). PAN dapat digunakan untuk komunikasi antara perangkat pribadi sendiri (komunikasi intrapersonal), seperti pada PC dengan *keyboard* ataupun *mouse*. Beberapa contoh alat yang digunakan dalam PAN adalah *printer*, mesin *fax*, *telephone*, PDA atau *scanner*. PAN dapat dihubungkan dengan kabel *computer buses* seperti USB dan *firewire*.

**Gambar 2.5** PAN (*Personal Area Network*)

**2. LAN (*Local Area Network*)**

Jaringan wilayah lokal (bahasa Inggris: *local area network* biasa disingkat LAN) adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 *Ethernet* menggunakan perangkat *switch*, yang mempunyai kecepatan *transfer*

data 10, 100, atau 1000 Mbit/s. Selain teknologi *Ethernet*, saat ini teknologi 802.11b (atau biasa disebut *Wi-fi*) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi *Wi-fi* biasa disebut *hotspot*.

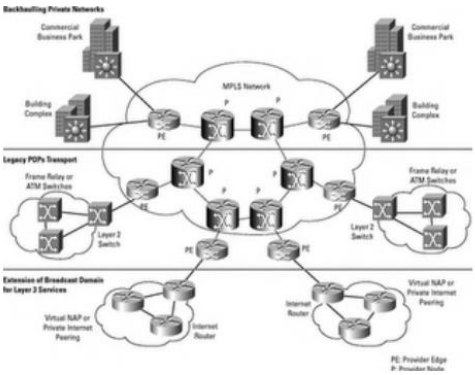



**Gambar 2.6** LAN (*Local Area Network*)

Pada sebuah LAN, setiap *node* atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep *dump* terminal. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti *printer*. Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai.

### 3. MAN (*Metropolitan Area Network*)

Jaringan wilayah metropolitan atau *Metropolitan area network* atau disingkat dengan MAN adalah suatu jaringan dalam suatu kota dengan *transfer* data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antar 10 hingga 50 km, MAN ini merupakan jaringan yang tepat untuk membangun jaringan antar kantor-kantor dalam satu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya.

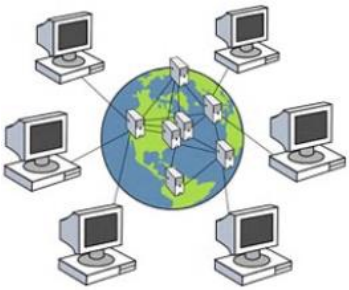



**Gambar 2.7** MAN (*Metropolitan Area Network*)

**4. WAN (*Wide Area Network*)**

*Wide Area Network* (WAN) adalah sebuah jaringan yang memiliki jarak yang sangat luas, karena radiusnya mencakup sebuah negara dan benua. WAN menggunakan sarana fasilitas transmisi seperti telepon, kabel bawah laut ataupun satelit. Kecepatan transmisinya beragam dari 2Mbps, 34 Mbps, 45 Mbps, 155 Mbps, sampai 625 Mbps (atau kadang-kadang lebih). Faktor khusus yang mempengaruhi desain dan *performance*-nya terletak pada siklus komunikasi, seperti jaringan telepon, satelit atau komunikasi pembawa lainnya.

Pada sebagian besar WAN, komponen yang dipakai dalam berkomunikasi biasanya terdiri dari dua komponen, yaitu kabel transmisi dan elemen *switching*. Kabel transmisi berfungsi untuk memindahkan *bit-bit* dari suau komputer ke komputer lainnya, sedangkan elemen *switching* disini adalah sebuah komputer khusus yang digunakan untuk menghubungkan dua buah kabel transmisi atau lebih. Saat data yang dikirimkan sampai ke kabel penerima, elemen *switching* harus memilih kabel pengirim untuk meneruskan paket-paket data tersebut.



**Gambar 2.8** WAN (*Wide Area Network*)

Jika dilihat dari fungsinya, sebenarnya WAN tidak jauh berbeda dengan LAN. WAN juga berfungsi sama seperti LAN mengkoneksikan antar komputer, *printer* dan juga *device* lainnya dalam satu jaringan. WAN pada dasarnya adalah kumpulan LAN yang ada diberbagai lokasi. Dibutuhkan sebuah *device* untuk menghubungkan antara LAN dengan WAN dan *device* tersebut adalah *router*.

## 2.9 Jaringan IdREN (*Indonesia Research Education Network*)

*IdREN* merupakan bagian dari REN (*Research and Education Networks*) yang terkoneksi melalui TEIN (*Trans Eurasia Information Networks*). *IdREN* diprakarsai oleh tim AdHoc dari 5 Perguruan Tinggi besar di Indonesia (ITB, UGM, UI, ITS dan UB) dengan dukungan penuh oleh Telkom. *IdREN* juga menyediakan berbagai aplikasi yang menunjang pengembangan riset serta pembelajaran bagi perguruan tinggi nasional.

## 2.10 OSPF (*Open Shortest Path First*)

*Open Shortest Path First* (OSPF) adalah sebuah protokol *routing* otomatis (*Dynamic Routing*) yang mampu menjaga, mengatur dan mendistribusikan informasi *routing* antar *network* mengikuti setiap perubahan jaringan secara dinamis. Pada OSPF dikenal sebuah istilah *Autonomus System* (AS) yaitu sebuah gabungan dari beberapa jaringan yang sifatnya *routing* dan memiliki kesamaan metode serta *policy* pengaturan *network*, yang semuanya dapat dikendalikan oleh *network* administrator. Dan memang kebanyakan fitur ini diguakan untuk managemen dalam skala jaringan yang sangat besar. Oleh karena itu

untuk mempermudah penambahan informasi *routing* dan meminimalisir kesalahan distribusi informasi *routing*, maka OSPF bisa menjadi sebuah solusi.

OSPF termasuk di dalam kategori IGP (*Interior Gateway Protocol*) yang memiliki kemapuan Link-State dan Alogaritma Djikstra yang jauh lebih efisien dibandingkan protokol IGP yang lain. Dalam operasinya OSPF menggunakan protokol sendiri yaitu protokol 89.

## 2.11 BGP (Border Gateway *Protocol*)

*Border Gateway Protocol* atau yang sering disingkat BGP merupakan salah satu jenis *routing protocol* yang ada di dunia komunikasi data. Sebagai sebuah *routing protocol*, BGP memiliki kemampuan melakukan pengumpulan rute, pertukaran rute dan menentukan rute terbaik menuju ke sebuah lokasi dalam jaringan. *Routing protocol* harus dilengkapi dengan algoritma yang pintar dalam mencari jalan terbaik. Namun yang membedakan BGP dengan *routing protocol* lain seperti misalnya OSPF dan IS-IS adalah BGP salah satu yang termasuk dalam kategori *routing protocol* jenis *Exterior Gateway Protocol* (EGP).

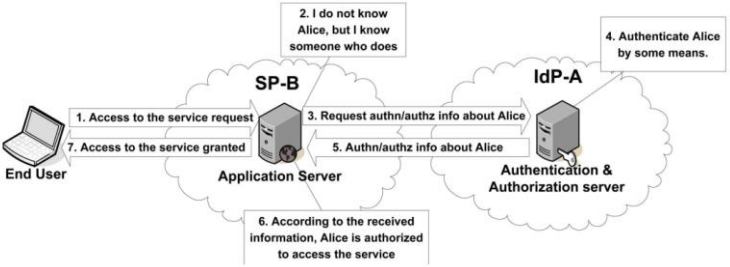
*Protocol* ini yang menjadi *backbone* dari jaringan internet dunia. BGP adalah protokol *routing* inti dari internet yg digunakan untuk melakukan pertukaran informasi *routing* antar jaringan. BGP dijelaskan dalam RFC 4271. RFC 4276 menjelaskan implementasi *report* pada BGP-4, RFC 4277 menjelaskan hasil uji coba penggunaan BGP-4. Ia bekerja dengan cara memetakan sebuah tabel IP *network* yang menunjuk ke jaringan yg dapat dicapai antar *Autonomous System* (AS). Hal ini digambarkan sebagai sebuah protokol *path vector*. BGP tidak menggunakan metrik IGP (Interior *Gateway Protocol*) tradisional, tapi membuat *routing decision* berdasarkan *path*, *network policies*, dan atau *rules set*. dari Januari 2006 hingga saat ini BGP versi 4 masih digunakan. BGP mendukung *Class Inter-Domain Routing* dan menggunakan *route aggregation* untuk mengurangi ukuran tabel *routing*. sejak tahun 1994, BGP-4 telah digunakan di internet. semua versi dibawahnya sudah tidak digunakan. BGP diciptakan untuk menggantikan protokol *routing* EGP yang mengijinkan *routing* secara tersebar sehingga tidak harus mengacu pada satu jaringan *backbone* saja.

### *2.12 Identity Federation*

Identity federation adalah mekanisme untuk menghubungkan identitas elektronik seseorang dan atribut, disimpan di beberapa sistem manajemen dengan identitas yang berbeda. *Identity federation* sangat relevan pada akhir-akhir ini dengan pertumbuhan yang pesat di dunia maya. *Identity federation* tersedia untuk pengguna, yang mana terafiliasi dengan *identity provider* (IdP), untuk mengakses *service provider* di kelompok yang kedua-*Service Provider* (SP). *Identity federation* menghubungkan antara *identity provider* dan *service provider*.

Untuk lebih mudah memahami bagaimana cara kerja *Identity federation* itu, mari dibuat sebuah contoh yang terlihat pada gambar 2.3. mahasiswi yang bernama Alice kuliah di Kampus A (IdP-A). Untuk proses registrasi, Alice memiliki akun email mahasiswa dengan identitas (alice@idp-a.edu) dan *password* . IdP-A termasuk *Identity federation*, sebuah organisasi/kelompok dari sebagian besar organisasi yang menawarkan autorisasi kepada pengguna. Dari sudut pandang Alice, organisasi ini adalah *Service Provider*. Misalkan, untuk meminta jaringan/layanan di *service Provider* B (SP-B). Pada langkah pertama dimulai dengan autentikasi oleh Alice (1). Ketika SP-B tidak mempunyai informasi tentang akun Alice tersebut (2). Maka diteruskan kepada IdP-A mengenai informasi akun Alice (3). Asumsikan Alice sedang melakukan autentikasi (4). Mentransmisikan informasi akun Alice (5), jadi SP-B dapat mengatur dan menentukan layanan kepada Alice (6). Jika proses autentikasi dan autorisasi berjalan lancar, Alice bisa menggunakan layanan tersebut (7).

Ada dua macam *Identity federation*, *Web-based Identity federation* dan *Authentication Authorization* and *Accounting* (AAA)-based *Identity federation*. Dari namanya jelas dua model tersebut masuk katagori layanan berbasis web.




**Gambar 2.9** Gambaran umum *Identity Federation*

### *2.13 Captive Portal*

Secara umum *captive portal* memiliki fungsi untuk mencegah atau memblokir koneksi yang tidak diinginkan dan mengarahkan *client* ke protokol tertentu, *captive portal* sebenarnya sama dengan *router* atau *gateway* yang memiliki fungsi untuk menyaring semua koneksi yang masuk dan menolak yang tidak diinginkan (*client* tidak terdaftar).

Pada saat seorang pengguna berusaha untuk melakukan *browsing* ke internet, *captive portal* akan memaksa pengguna yang belum terautentikasi untuk menuju ke *autentication web* dan akan diberi *prompt login* termasuk informasi tentang *hotspot* yang sedang digunakan.

Cara kerja *captive portal* adalah sebagai berikut :

1. *User* dengan *wireless client* diizinkan untuk terhubung *wireless* untuk mendapatkan *IP address* (DHCP).
2. *Block* semua *traffic* kecuali yang menuju ke *captive portal* (registrasi/otentikasi berbasis *web*) yang terletak pada jaringan.
3. *Redirect* atau belokkan semua *traffic web* ke *captive portal*.
4. Setelah *user* melakukan registrasi atau *login*, izinkan akses ke jaringan (internet).

### 2.14 *Remote Authentication Dial In User Service* (RADIUS)

RADIUS (*Remote Access Dial-in User Service*) adalah salah satu mekanisme untuk melakukan akses kontrol dalam mengecek dan melakukan autentikasi yang sebelumnya sudah banyak dilakukan, yaitu menggunakan metode response/challenge. RADIUS dikembangkan pada pertengahan tahun 1990 oleh *Livingstone Enterprise* (sekarang *Lucent Technologies*). Pada awal perkembangannya RADIUS menggunakan *port* 1645, namun *port* tersebut bentrok dengan layanan *datametrics*. Sehingga *port* RADIUS diganti dan sekarang *port* yang digunakan oleh RADIUS adalah *port* 1812 dengan format standarnya ditetapkan pada RFC (*Request for Command*) 2138.

Server RADIUS memiliki mekanisme keamanan untuk melakukan autentikasi dan autorisasi kepada pengguna sebelum melakukan koneksi. Pada saat komputer klien ingin melakukan koneksi jaringan, maka server RADIUS akan melakukan autentikasi terlebih dahulu dengan meminta identitas pengguna yang merupakan *username* dan *password*

untuk dicocokkan dengan data yang terdapat dalam *database* server RADIUS. Selanjutnya RADIUS akan menentukan apakah pengguna dapat menggunakan layanan jaringan komputer atau tidak. Jika proses autentikasi sukses dilakukan maka akan dilakukan proses pelaporan yaitu mencatat semua aktivitas koneksi dan jumlah transfer data yang dilakukan oleh pengguna di dalam jaringan. Proses pelaporan server RADIUS terhadap pengguna jaringan bisa dalam bentuk waktu (detik, menit, jam) maupun dilakukan dalam bentuk besar transfer data (*byte*, *Kbyte*, *Mbyte*).

RADIUS merupakan protokol yang dikembangkan untuk melakukan proses AAA (*Authentication*, *Authorization*, and *Accounting*). Berikut merupakan RFC (*Request for Command*) yang berhubungan dengan RADIUS :

1. RFC 2548 : *Microsoft Vendor-Spesific* RADIUS *Attributes*
2. RFC 2865 : *Remote Authentication Dial-In User Service* (RADIUS)
3. RFC 2866 : RADIUS *Accounting*
4. RFC 2867 : RADIUS *Accounting* for Tunneling
5. RFC 2868 : RADIUS *Authentication* for Tunneling
6. RFC 2869 : RADIUS *Extensions*
7. RFC 3162 : RADIUS *over* Ipv6

RADIUS pada umumnya digunakan oleh penyedia layanan internet atau ISP (*Internet Service Provider*) untuk melakukan *Authentication* (pembuktian keaslian pengguna), *Authorize* (mengatur pemberian hak/otoritas) dan *Accounting* (mencatat pengguna layanan yang digunakan).

### 2.14.1 Gambaran Mengenai AAA

RADIUS dibangun dengan kerangka kerja yang dikenal dengan proses AAA, yaitu terdiri dari *Authentication* (pembuktian keaslian), *Auhtorize* (pemberi hak/otoritas) dan *Accounting* (akuntansi). Service model ini digunakan untuk melaporkan dan mengatur semua transaksi dari mulai awal menggunakan jaringan hingga selesai menggunakan jaringan. Arsitektur AAA merupakan strategi yang lebih baik daripada yang lainnya. Sebelum diperkenalkan AAA, telah digunakan peralatan individu untuk melakukan autentikasi para pengguna. Namun tanpa standar yang formal, masing-masing mesin memiliki sistem autentikasi

yang berbeda-beda, mungkin saja menggunakan autentikasi CHAP (*Challenge*/*Handshake Authentication Protocol*) sedangkan yang lainnya menggunakan profile. Dan yang lainnya lagi menggunakan query *databases* internal dengan SQL. Masalah utama ketika menggunakan model yang tidak beraturan seperti ini adalah skalabilitas salah satunya.

Untuk menciptakan arsitektur yang fungsional dibentuk kelompok AAA oleh IETF yang akan memetakan keterbatasan dari sistem yang digambarkan di atas. Sebenarnya terdapat kebutuhan untuk memusatkan peralatan dan monitoring pengguna pada jaringan komputer yang beragam. Sehingga ISP-ISP mulai menawarkan tidak hanya *dial up*, akan tetapi mulai menawarkan ISDN, xDSL dan koneksi menggunakan kabel modem. Oleh sebab itulah diperlukan suatu cara standar agar dapat memverifikasi para pengguna untuk masuk ke dalam suatu sistem dan memonitoring melalui jaringan. Karena kebutuhan tersebut dan melalui sebuah proses maka lahirlah arsitektur AAA.

Model arsitektur AAA berfokus pada tiga aspek yang paling penting dari kontrol akses pengguna yaitu autentikasi, autorisasi dan akuntansi.

1. *Authentication*

   *Authentication* merupakan proses yang digunakan untuk melakukan verifikasi terhadap identitas yang digunakan pengguna untuk dapat masuk ke dalam suatu sistem atau service menggunakan *username* dan *password* , dan seperti yang kita ketahui *password* akan mewakili bagaimana pengguna akan diverifikasi. Jika *password* sampai diketahui oleh pihak lain maka hal tersebut akan menghancurkan metode *Authentication* dimana orang yang tidak berhak dapat masuk ke dalam suatu sistem. Dalam situs *e-commerce* dan situs-situs internet bisnis lainnya, membutuhkan *Authentication* yang jauh lebih kuat dan dapat dipercaya. Secara digital sertifikasi merupakan salah satu solusinya dan mungkin 5 sampai 10 tahun ke depan sertifikasi secara digital akan menjadi bagian dari PKI (*Public Key Infrastructure*) yang menjadi rekomendasi *Authenticator* di internet.

2. *Authorization*

   *Authorization* merupakan aturan pengguna yang memutuskan apa saja yang dapat dilakukan oleh pengguna yang telah melakukan autentikasi dalam suatu sistem. Sebagai contoh, dalam

kasus ISP, ISP akan memutuskan untuk memberikan alamat IP (*Internet Protocol*) dari hasil DHCP atau alamat IP *static*. Untuk mendefinisikan peraturan ini dilakukan oleh seorang sistem administrator.

3. *Accounting*

   Bagian terakhir dari kerangka kerja AAA adalah *Accounting*. *Accounting* dapat mencatat dan mengukur sumber daya yang digunakan, termasuk jumlah data yang dikirim dan diterima pelanggan selama memanfaatkan sumber daya, jumlah waktu yang digunakan dan besarnya kecepatan pengguna pelanggan. Sistem *Accounting* terselenggara oleh penggunaan informasi dan pembukuan *statistic* serta digunakan untuk kegiatan kendali pemberian hak (otoritas), analisa *trend* (kecenderungan), billing, rencana kapasitas dan pemanfaatan sumber daya.

### 2.14.2 Format Paket Data RADIUS

Pada format paket data RADIUS terdiri dari 5 bagian yaitu *Code*, *Identifier*, *Length*, *Authenticator* dan *Attributes* seperti yang ditunjukkan pada gambar 2.8 di bawah ini :


**Gambar 2.10** Struktur Paket Data RADIUS

1. *Code*

   *Code* digunakan untuk membedakan tipe pesan yang dikirim RADIUS dan memiliki panjang 1 *byte* (8 bit). Tipe pesan RADIUS dapat berupa *access accept*, *access request*, *access challenge* dan *access reject*.

2. *Identifier*

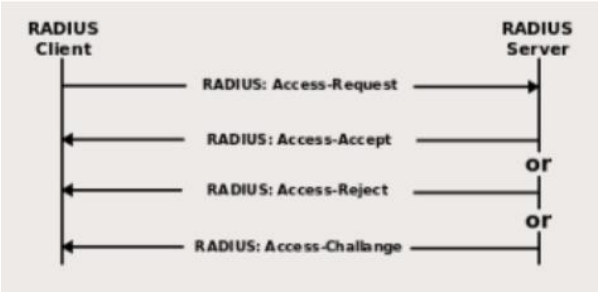
   *Identifier* digunakan untuk menyesuaikan antara paket data permintaan dengan paket respon dari server RADIUS dan mempunyai panjang 1 *byte* (8 bit).

3. *Length*
   *Length* digunakan untuk memberikan informasi mengenai panjang paket dan panjang l*ength* adalah 2 *byte*. Apabila paket kurang atau lebih daripada yang diidentifikasikan pada l*ength* maka paket tersebut akan dibuang.
4. *Authenticator*
   *Authenticator* digunakan untuk melakukan autentikasi tanggapan dari server RADIUS dan memiliki panjang 16 *byte*.
5. *Attributes*
   *Attributes* berisi autentikasi, autorisasi dan informasi, panjang yang dimiliki oleh *attributes* tidak tetap. Contoh dari *attributes* RADIUS adalah *username* dan *password* .

### 2.14.3 Prinsip Kerja RADIUS

RADIUS bekerja sebagai *protocol security* dengan menggunakan sistem *client-server* terdistribusi yang digunakan bersamaan AAA untuk mengamankan jaringan dari pengguna yang tidak berhak. Dalam melakukan autentikasi *user*, RADIUS melakukan serangkaian komunikasi antara *client* dan server. Bila *user* berhasil melakukan autentikasi maka *user* akan dapat menggunakan layanan yang disediakan jaringan. Prinsip kerja RADIUS dapat diilustriasikan sebagai berikut :

1. Prinsip kerja RADIUS sebagai *Authentication* dan *Authorization*

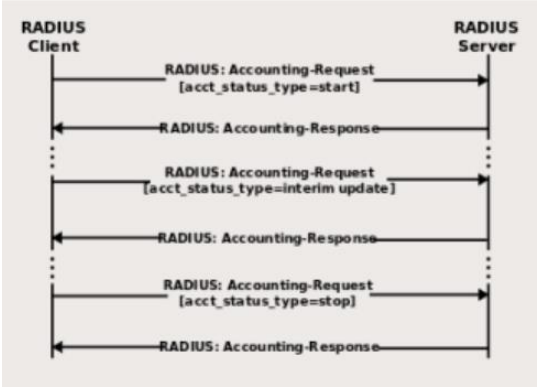



**Gambar 2.11** Ilustrasi RADIUS sebagai *Authentication* dan *Authorization*

Dari ilustrasi gambar di atas dapat dijelaskan sebagai berikut :

1. Pertama *user* mengirimkan *request* kepada *Remote Access Server* (RAS)
2. Kemudian RAS mengirimkan pesan RADIUS *Access request* kepada RADIUS server untuk meminta *Authorization* dengan memberikan akses melalui *protocol* RADIUS. *Request* yang dikirimkan oleh RAS mengandung identitas *user* seperti *username* , *password* , IP *address* dan lain-lainnya.
3. RADIUS server melakukan pengecekan apakah informasi yang dikirim RAS benar menggunakan *authentication schemes* seperti EAP, CHAP dan PAP.
4. Dari proses tersebut terdapat tiga respon pada RADIUS server, yaitu :
   a. *Accept* (*user* telah mendapatkan akses)
   b. *Reject* (*user* gagal melakukan verifikasi)
   c. *Challenge* (verifikasi terhadap *user* belum dapat diselesaikan oleh RADIUS server)

2. Prinsip kerja RADIUS sebagai *Accounting*
   Setelah *user* berhasil melakukan autentikasi dan masuk ke dalam jaringan, maka akan dimulai proses *Accounting*.



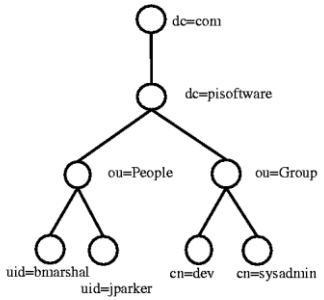

**Gambar 2.12** Ilustrasi Prinsip Kerja RADIUS sebagai *Accounting*

Dari ilustrasi gambar di atas terdapat 3 tipe *request user* pada *Accounting*, yaitu :

1. *Acct-Status-Type attribute* dengan *value* "*start*". Pesan tersebut dikirim oleh NAS kepada RADIUS server sebagai sinyal bahwa *user* telah memulai akses jaringan.
2. *Acct-Status-Type attribute* dengan *value* "*interim update*". Ini merupakan *update status user*.
3. *Acct-Status-Type attribute* dengan *value* "*stop*". Ini merupakan sinyal yang dikirim ke RADIUS server bahwa *user* telah berhenti melakukan koneksi.

## 2.15 LDAP (*Light Directory Access Protocol*)

LDAP (*Lightweight Directory Access Protocol*) adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori (*Directory Service*) yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang *people*, *Organizations*, *roles*, *service*s dan banyak entitas lainnya. LDAP menggunakan model *Client-Server*, dimana *Client* mengirimkan *Identifier* data kepada *Server* menggunakan protokol TCP/IP dan *Server* mencoba mencarinya pada DIT (*Directory Information* Tree) yang tersimpan di *Server*. Bila di temukan maka hasilnya akan dikirimkan ke *Client* tersebut namun bila tidak maka hasilnya berupa *pointer* ke *Server* lain yang menyimpan data yang di cari.

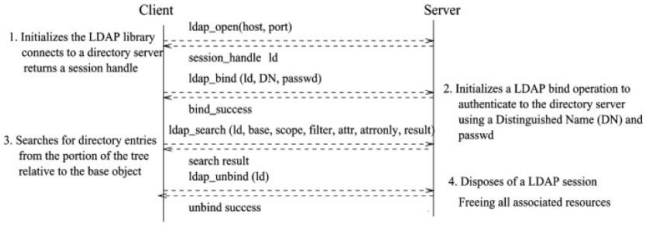



**Gambar 2.13** Model *Directory* LDAP

Gambar 2.13 menunjukkan model dari struktur sebuah *Directory*. Secara prinsip struktur *database* pada suatu *Directory service* adalah

hierarki seperti yang di tunjukkan pada gambar di atas. Suatu *Directory service* akan memiliki item yang di jadikan sebagai *root*. Untuk sebuah titik *root*, secara umum di tunjukkan dengan suatu attribut dc (*Domain Component*) atau o (*Organization*) mungkin juga ou (*Organization* Unit). Kemudian pada titik daun (*leaf*) biasanya akan berisi item dengan attribut uid (*User* ID) ataupun cn (*Common Name*). *Directory service* biasanya menyimpan informasi dalam bentuk struktur *tree* yang dinamakan *Directory Information* (DIT).

Informasi pada LDAP disimpan dalam suatu data yang memiliki beberapa atribut. Jika pada *relational database* memiliki *primary key* untuk membedakan antar data, maka pada LDAP memiliki *Distinguished Name* (DN) yang bernilai unik untuk tiap data. DN didapat dengan mengurutkan lokasi data dari *root* DIT sampai direktori data tersebut.




**Gambar 2.14** Proses autentikasi pada LDAP

LDAP mengakses *Directory Service* yang merupakan perangkat lunak yang menyimpan, mengorganisir dan menyediakan akses ke informasi dalam sebuah direktori. Terdapat perbedaan *Directory Service* dengan *Relational Database* , yaitu penggunaan DS lebih ke proses pembacaan data daripada penulisan data. Karena DS lebih sederhana hanya menyimpan data *username* , *password* , dan beberapa data penting saja, serta tidak mendukung proses transaksi rumit yang biasanya ditemukan pada *Relational Database* seperti MySQL.

## 2.16 *FreeRADIUS*

*FreeRADIUS* merupakan modular yang dikembangkan untuk dapat bekerja dengan performa tinggi dan didistribusikan di bawah lisensi GNU (*General Public License*). *FreeRADIUS* bisa diunduh dan digunakan secara gratis. Meskipun gratis, di dalam *FreeRADIUS* sudah mengandung RADIUS server, PAM, modul *Apache* dan banyak tambahan *tool* lainnya.

*FreeRADIUS* adalah RADIUS server yang paling banyak digunakan di dunia dan menjadi RADIUS server yang paling populer di kalangan *OpenSource*. *FreeRADIUS* su*port* dengan semua protokol autentikasi dan dilengkapi dengan web administrasi pengguna berbasis PHP yang disebut *dialupadmin*. *FreeRADIUS* juga mengandung AAA yang dibutuhkan oleh banyak perusahaan seperti perusahaan telekomunikasi. *FreeRADIUS* juga merupakan server yang cepat dan memiliki banyak fitur.

*FreeRADIUS* dikembangkan oleh Alan Dekok dan Miquel mengembangkan *Cistron* RADIUS server, namun tidak dikembangkan lagi. Seiring perkembangan waktu *FreeRADIUS* terus dikembangkan dan su*port* dengan banyak fitur selain sup*port* teks file juga su*port* LDAP, MySQL, PostgreSQL, Oracle dan banyak fitur lainnya. Fitur *FreeRADIUS* secara garis besar adalah sebagai berikut :

1. Mempunyai *performance* yang tinggi dan mendukung HA, *Fail-Over*
2. Mendukung banyak *operating system*, kaya fitur, EAP, *Database* , fungsionalitas AAA, *virtual server*, *proxy*, dan lainnya.
3. Skalabilitas, untuk beban yang tinggi *FreeRADIUS* mendukung berdasarkan maksimum *request* dan maksimum server.
4. Modular, mendukung *addon/plugin* tambahan dan dapat diimplementasikan pada *embedded system*.

Alasan utama banyak yang memilih *FreeRADIUS* adalah mahalnya harga RADIUS server komersial. Sebagai contoh : harga *interlink's secure* XS mulai dari $2375 untuk 250 pengguna, *funk odyssey* server $2500, VOP Radius *Small Business* mulai dari $995 untuk 100 pengguna. Harga RADIUS server komersial tersebut tidak terjangkau untuk pengguna hotspot, terutama untuk kampus.

Salah satu contoh RADIUS server non-komersial adalah *FreeRADIUS*. *FreeRADIUS* tidak kalah dengan RADIUS server komersial. Salah satu buktinya *FreeRADIUS* sudah mendukung beberapa *Access point* (AP)/*Network Access Server* (NAS) di bawah ini:

1. 3Com/USR *Hiper Arc Total Control*
2. 3Com/USR *Total Control*
3. 3Com/USR *Netserver*
4. *Ascend Max* 4000 *family*

5. *Cistron PortSlave*
6. Cisco *Access Server family*
7. Computone PowerRack
8. Livingston *Port*Master
9. Cyclades PathRAS
10. Patton 2800 family
11. Multitech CommPlete Server

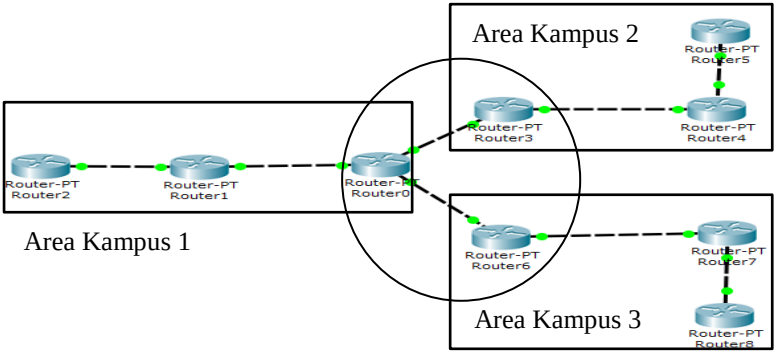
Selain *FreeRADIUS*, terdapat beberapa RADIUS server non-komersial lainnya, diantaranya adalah sebagai berikut :

1. Cistron RADIUS Server
   Cistron RADIUS dibuat oleh Miguel van Smoorenburg yang merupakan *free software* di bawah lisensi GNU GPL.
2. ICRADIUS
   ICRADIUS merupakan varian dari Cistron dan menggunakan MySQL untuk menyimpan *database* nama dan *password* pengguna serta berbasis web, sehingga akan memudahkan administrator untuk mengelolah server ini.
3. JRADIUS
   Merupakan Java *plugin* untuk *FreeRADIUS*.
4. XtRADIUS
   XtRADIUS adalah *software* RADIUS server yang berbasiskan pada Cistron RADIUS. Perbedaan utama dari XtRADIUS dengan RADIUS server lainnya adalah kita dapat mengeksekusi *script* untuk menangani autentikasi.
5. OpenRADIUS
   OpenRADIUS dapat berjalan di beberapa sistem operasi UNIX. OpenRADIUS merupakan *software* gratis yang dapat dilakukan modifikasi bila dianggap perlu.
6. YARDRADIUS
   YARDRADIUS merupakan *software* gratis yang berasal dari open source Livinston RADIUS server 2.1. YARDRADIUS dibaca Y-A-R-D RADIUS merupakan singkatan dari Yet Another Radius Daemon RADIUS

*Halaman ini sengaja dikosongkan*

# BAB III
# PERANCANGAN DAN REALISASI ALAT

Perancangan sistem pada tugas akhir ini yaitu merancang *Test bed* jaringan IdREN terlebih dahulu. *Test bed* jaringan IdREN ini terdiri dari jaringan utama dan jaringan di bawahnya. Jaringan utama yang dimaksud di sini merupakan jaringan yang menghubungkan lima kampus besar di Indonesia, yaitu UI, ITB, UGM, ITS, dan UB. Jaringan utama IdREN ini menggunakan *routing protocol* BGP. Jaringan yang di bawahnya merupakan jaringan kampus yang berada di daerah kelima kampus tersebut. Jadi jaringan kampus tersebut akan terkoneksi dengan jaringan utama IdREN dengan *routing protocol* OSPF. Pada tugas akhir ini hanya menggunakan tiga area kampus dikarenakan ketersediaan *router* cisco yang terdapat di laboratorium B301. Area kampus 1 diasumsikan area kampus ITB, area kampus 2 diasumsikan area kampus ITS, dan area kampus 3 diasumsikan area kampus UGM. Pada gambar 3.1 terlihat *Test bed* jaringan IdREN.




**Gambar 3.1** *Test bed* jaringan IdREN

## 3.1 Perancangan

Proses perancangan sistem pada tugas akhir ini dibagi dalam tiga tahap. Berikut tahapan perancangan sistem :

1. Perancangan *Test bed* jaringan IdREN
2. Perancangan *server* untuk autentikasi dan database akun
3. Perancangan keamanan *Test bed* jaringan IdREN

Secara umum sistem memusatkan proses autentikasi dan penyimpanan database dalam satu *server*. Karena itu *server* autentikasi dan *server* database harus dilakukan instalasi dan konfigurasi hingga *server* tersebut dapat terhubung dengan *Test bed* jaringan IdREN.

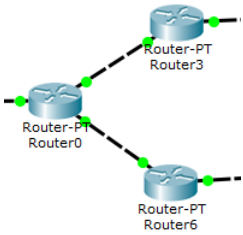
### 3.1.1 Perancangan *Test bed* Jaringan IdREN

*Test bed* jaringan IdREN memiliki dua jaringan, yaitu jaringan utama dan jaringan dibawahnya. Jaringan utama menghubungkan router antar area kampus. Jaringan dibawahnya menghubungkan router di setiap area kampus. Metodologi yang digunakan di *Test bed* jaringan IdREN yaitu menggunakan *routing protocol* BGP dan *routing protocol* OSPF. *Routing protocol* BGP digunakan untuk menghubungkan *router* antar area kampus 1, area kampus 2 dan area kampus 3. *Routing protocol* OSPF digunakan untuk menghubungkan *router* dalam setiap area kampus.

Pada tabel 3.1 dijelaskan mengenai pengalamatan masing-masing *router* di *Test bed* jaringan IdREN. Jaringan utama IdREN menggunakan *routing protocol* BGP yang terjadi pada *router* 0, *router* 3, dan *router* 6.

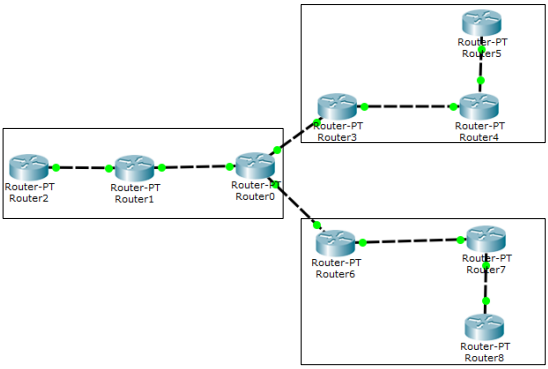
**Tabel 3.1** Pengalamatan Tiap-Tiap *Router*

| *Router* | IP *loopback* | IP Port fa0/0 | IP port fa0/1 | *Routing Protocol* |
|---|---|---|---|---|
| *Router* 0 | 1.1.1.1 | 192.168.1.1 | 172.192.100.1 | OSPF. BGP |
| *Router* 1 | 2.2.2.2 | 192.168.1.2 | 192.168.2.1 | OSPF |
| *Router* 2 | 3.3.3.3 | | 192.168.2.2 | OSPF |
| *Router* 3 | 4.4.4.4 | 192.168.3.1 | 172.192.100.2 | OSPF, BGP |
| *Router* 4 | 5.5.5.5 | 192.168.3.2 | 192.168.4.1 | OSPF |
| *Router* 5 | 6.6.6.6 | | 192.168.4.2 | OSPF |
| *Router* 6 | 7.7.7.7 | 192.168.5.1 | 172.192.100.3 | OSPF, BGP |
| *Router* 7 | 8.8.8.8 | 192.168.5.2 | 192.168.6.1 | OSPF |
| *Router* 8 | 9.9.9.9 | | 192.168.6.2 | OSPF |




**Gambar 3.2** *Router* yang Menggunakan BGP

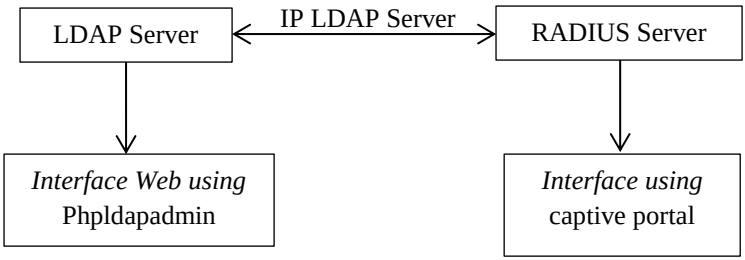
Diasumsikan *router* 0 yaitu *router* di ITB, *router* 3 diasumsikan *router* di ITS, dan *router* 6 diasumsikan *router* di UGM. Terdapat tiga wilayah/area yang berbeda. Pertama di Bandung, kedua di Surabaya, ketiga di Jogjakarta. Untuk perguruan tinggi yang ada di tiga wilayah tersebut, maka mereka harus menggunakan *routing protocol* OSPF. *Routing protocol* ini digunakan karena bisa digunakan pada vendor apapun. Jadi tanpa perlu menyamakan *router* pada tiap-tiap perguruan tinggi, mereka bisa terhubung pada jaringan IdREN dengan *routing protocol* OSPF.




**Gambar 3.3** Daerah yang menggunakan OSPF

### 3.1.2 Perancangan *Server*

Sistem autentikasi terpusat *Identity Federation* harus dilakukan perancangan terlebih dahulu untuk memudahkan pada saat tahap implementasi sistem, dilakukan perancangan menggunakan protokol LDAP dan RADIUS yang dikombinasikan dengan aplikasi *web* sebagai interface.

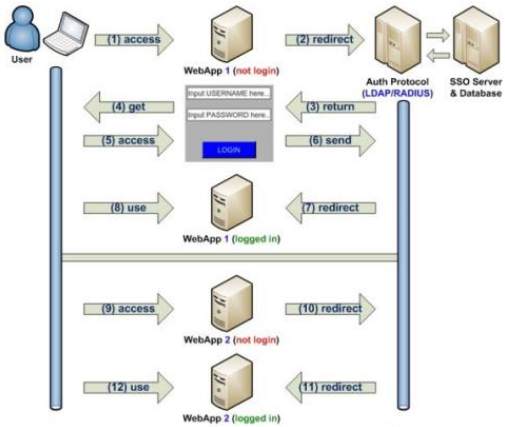



**Gambar 3.4** Gambaran Umum Perancangan *Server*

Pada gambar 3.4 menunjukkan gambaran umum perancangan *server* antara RADIUS *server* dengan LDAP *server*. Setiap *server* memiliki interface untuk memudahkan dalam mengelolah sebuah *server*. LDAP digunakan sebagai *server* database. LDAP *server* dibantu oleh OpenLDAP yang berfungsi untuk menyimpan akun *login* pengguna. Interface pada LDAP *server* menggunakan software yang berbasis web yaitu Phpldapadmin.

RADIUS *server* berfungsi untuk meneruskan paket data akun dari LDAP *server* ke pengguna. *Software* yang digunakan sebagai RADIUS *server* adalah *free*RADIUS. RADIUS *server* terhubung dengan LDAP *server* menggunakan perintah yang menunjukkan alamat ip dari LDAP *server*. Setiap RADIUS *server* bisa terhubung dengan lebih dari satu LDAP *server*. Hal ini yang dinamakan dengan *sharing authority* di *Test bed* jaringan IdREN. Untuk mengetahui apakah RADIUS *server* sudah terhubung dengan LDAP *server* digunakan sebuah perintah *radtest*. Perintah ini berisi agar data dapat diambil dari LDAP *server* oleh RADIUS *server*.

*Captive portal* memiliki beberapa tujuan yaitu menguji proses autentikasi, sebagai tampilan *interface*, dan untuk menahan pengguna dari jaringan lokal ke jaringan publik. *Captive portal* yang digunakan dalam tugas akhir ini yaitu coovachilli. *Captive portal* akan terhubung dengan RADIUS *server* untuk mengambil data dari LDAP *server*. *Captive portal* yang terpasang di komputer *server* harus memiliki syarat, adalah komputer *server* harus memiliki dua *ethernet*. *Ethernet* pertama digunakan untuk terhubung dengan jaringan internet. Sedangkan *ethernet* kedua digunakan untuk terhubung dengan jaringan lokal.




**Gambar 3.5** Rancangan *Identity Federation* yang dibangun

### 3.1.3 Perancangan Keamanan

Perancangan *Security* dari sistem dengan menggunakan protokol *Hypertext Transfer Protocol Secure* (HTTPS) dalam komunikasi RADIUS *Server* dengan aplikasi *client*. RADIUS *Server* menggunakan *layer Security Security* Socket *Layer* (SSL) dengan membangun *self signed certificate* dibagian *server* serta meyakinkan semua *client* yang berada dalam lingkungan tersebut dapat berkomunikasi secara *Secure* dengan sertifikat tersebut.

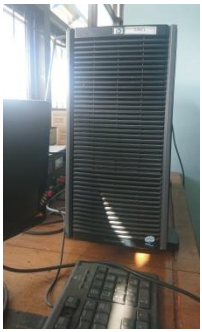
Koneksi *Secure* SSL terjadi diantara aplikasi *client* dengan RADIUS *server* ketika proses autentikasi. Sedangkan komunikasi antara RADIUS *server* dengan LDAP *server* berada pada lingkungan yang *Secure* karena *user* tidak diijinkan melakukan komunikasi langsung ke *server* LDAP.

## 3.2 Peralatan Pendukung

Untuk mendukung proses implementasi dan pengujian penelitian ini dibutuhkan peralatan pendukung seperti perangkat keras dan perangkat lunak yang digunakan. Sistem ini dirancang sebagai simulasi autentikasi yang bekerja menggunakan satu *server* yang dipasang di komputer laboratorium dan satu laptop *client* milik penulis, kemudian dihubungkan menggunakan koneksi kabel LAN.

### 3.2.1 Perangkat Keras

Dalam Tugas Akhir ini digunakan satu komputer *server* yang berada di laboratorium Telekomunikasi dan Jaringan B301. Satu komputer *server* terdiri dari dua *server*, yaitu *server* RADIUS dan *database server* LDAP. Komputer *server* yang berada di lab B301 terdiri dari dua *ethernet*. *Ethernet* pertama digunakan untuk jaringan lokal sedangkan *ethernet* kedua digunakan untuk jaringan publik.



**Gambar 3.6** *Server* Untuk Tugas Akhir

Untuk *Test bed* jaringan IdREN menggunakan beberapa komponen, antara lain sebagai berikut :

1. *Router* Cisco
2. Kabel UTP *Cross*
3. Kabel Serial to USB

Untuk *Test bed* jaringan utama IdREN menggunakan *routing protocol* BGP sedangkan jaringan dibawahnya menggunakan *routing protocol* OSPF. Kabel yang digunakan untuk menghubungkan *router* yaitu kabel UTP *cross*. Kabel UTP *cross* digunakan karena menghubungkan satu device yang sama. Jika ingin menghubungkan *device* yang berbeda menggunakan kabel UTP *straight*. Kabel yang digunakan untuk memasukkan perintah dari komputer ke *router* menggunakan kabel serial to usb.

### 3.2.2 Perangkat Lunak

Pada komputer *server* yang berada di laboratorium Telekomunikasi dan Jaringan B301 terdapat beberapa perangkat lunak yang sudah terinstal, berikut adalah perangkat lunaknya :

1. Sistem Operasi Ubuntu *Server* 16.04

   Pada komputer yang akan menjalankan *server* RADIUS dan *database server* LDAP telah tertanam sistem operasi ubuntu berbasis Linux 64 bit. Ubuntu merupakan salah satu distribusi Linux berbasis Debian dan didistribusikan sebagai perangkat lunak bebas. Ubuntu versi ini dirancang untuk kepentingan penggunaan *server*.
2. OpenLDAP

   Perangkat lunak yang bersifat *opensource* untuk menjalankan *database server* sebagai pengelola direktori *database*. Perangkat lunak ini release terbaru dengan versi openldap 2.4.4
3. PHPLDAPAdmin

   Selain OpenLDAP di dalam *database server* LDAP juga terdapat PHPLDAPAdmin sebagai antarmuka pengelolaan *database* khusus LDAP berbasis web dengan versi 1.2
4. FreeRADIUS

   FreeRADIUS adalah perangkat lunak yang bersifat *opensource* untuk menjalankan *server* RADIUS, versi yang digunakan yaitu FreeRADIUS 2.2.7
5. CoovaChilli

   CoovaChilli merupakan perangkat lunak *captive portal* gratis pengembangan dari chillispot. Pada sistem ini digunakan coovachilli versi 1.3.0
6. PHP 5

   PHP adalah bahasa pemrograman dengan semua sintaks yang diberikan akan sepenuhnya dijalankan pada *server* dan hasilnya dikirimkan ke browser. Versi PHP yang digunakan dalam tugas akhir ini adalah PHP versi 5.
7. Putty

   Putty adalah aplikasi terminal akses yang digunakan untuk membuat *remoteconnection* komputer melalui *port* SSH atau sebagainya.

## 3.3 Pengujian

Pada tahap pengujian dilakukan bila konfigurasi jaringan dan *server* harus sudah jadi. Tahap pengujian bertujuan untuk mengetahui apakah jaringan IdREN sudah terhubung dengan *server*. Pengujian menggunakan *iperf*. *Iperf* digunakan untuk menguji performa unjuk

kerja jaringan dengan membangkitkan layanan komunikasi TCP dan UDP *client-server*.

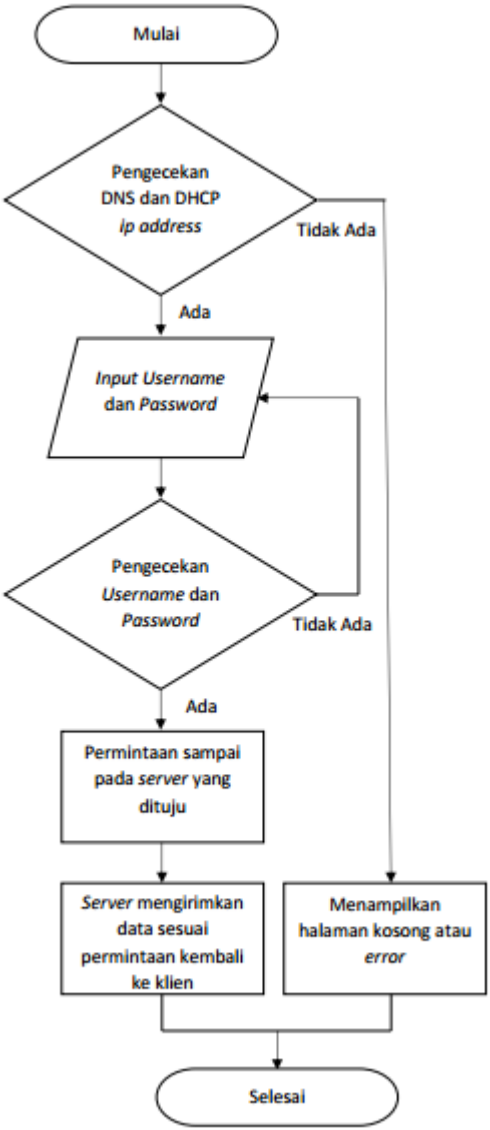
Pengujian keamanan menggunakan aplikasi *wireshark*. *Wireshark* adalah tool yang ditujukan untuk melakukan analisa paket data jaringan. *Wireshark* melakukan monitoring secara *real-time* selanjutnya *wireshark* melakukan penangkapan data dan menampilkannya selengkap mungkin.

Pengujian menggunakan *ping* yang bertujuan untuk memeriksa konektivitas antar jaringan melalui sebuah *Transmission Control Protocol*/*Internet Protocol* (TCP/IP) dengan cara mengirim sebuah paket *internet control message protocol* (ICMP) kepada alamat ip yang hendak diuji coba konektivitasnya.

Pengujian *server* dengan menuliskan alamat *url* di *web browser*. Dengan begitu pengguna akan langsung di-*direct* ke proses autentikasi sebelum menggunakan layanan internet. Setelah pengguna dapat masuk ke *Test bed* jaringan IdREN, akan muncul jendela baru yang digunakan untuk keluar/*logout*. Pengujian koneksi antara RADIUS *server* dengan LDAP *server* menggunakan perintah *radtest*. *Radtest* adalah perintah untuk mengirimkan data dari LDAP *server* menuju RADIUS *server*.

### 3.4 Implementasi Sistem

Pada tahap implementasi sistem, *server* menggunakan Linux Ubuntu dan *client* menggunakan windows, kemudian melakukan instalasi perangkat lunak yang dibutuhkan. Setelah itu *server* dan *client* dihubungkan dalam satu jaringan. Semua aplikasi di *server* dipastikan sudah berjalan dengan lancar. Aplikasi *web* diakses dari *client* dengan mengetik IP *address server* pada *browser*. Pada gambar 3.7 menunjukkan diagram alir sistem autentikasi yang digunakan di tugas akhir ini.



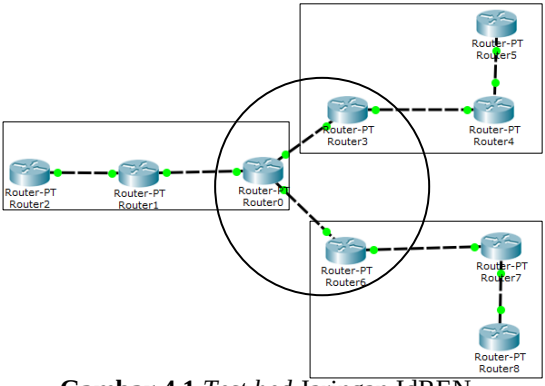

**Gambar 3.7** Diagram alir sistem *Identity Federation*

*Halaman ini sengaja dikosongkan*

# BAB IV
# PENGUJIAN DAN ANALISA DATA

## 4.1 Pembuatan *Test Bed* Jaringan IdREN

Pada *test bed* jaringan IdREN terdapat dua *routing protocol*, yaitu *routing protocol* BGP dan *routing protocol* OSPF. *Routing protocol* BGP digunakan pada jaringan utama IdREN, sedangkan *routing protocol* OSPF digunakan pada jaringan di bawahnya. Di gambar 4.1 menunjukkan *test bed* jaringan IdREN. Terdapat sembilan buah *router* yang digunakan. Untuk pengalamatan ip *address* pada masing-masing *port* di setiap *router* sudah dijelaskan pada bab 3 beserta *router* mana yang menggunakan *routing protocol* OSPF dan BGP.




**Gambar 4.1** *Test bed* Jaringan IdREN

Langkah pertama yang dilakukan yaitu meyiapkan *router* seperti pada gambar 4.1. Semua *router* dihubungkan dengan kabel *cross*. Setelah semua *router* tersambung, selanjutnya adalah konfigurasi *router* pada masing-masing area. Terdapat tiga area, area sebelah kiri dinamakan area 10, area atas dinamakan area 20, area bawah dinamakan area 30. Pada gambar 4.2 ditunjukkan *list* program untuk *router* 0 sampai *router* 8, *list* program ini berisi memberikan perintah pada masing-masing *interface*. Pertama memberikan alamat pada *interface loopback*0. *Interface loopback* adalah *interface logic* bukan fisik jadi *loopback* tidak memiliki kabel fisik yang terhubung ke *router*. Untuk *router* 1 dan *router* selanjutnya, alamat ip untuk *interface loopback*

adalah 2.2.2.2, 3.3.3.3, dst. Kedua memberikan alamat pada *interface fastethernet0/0*. Sesuaikan alamat ip seperti tabel 3.1. Memasukkan perintah "*no shutdown*" agar *interface* tersebut tetap menyala setelah memberikan alamat.

```
Router> en
Router# conf t
Router(config)# int lo0
Router(config-if)# ip addr 1.1.1.1 255.255.255.255
Router(config-if)# ex
Router(config)# int fa0/0
Router(config-if)# ip addr 192.168.1.1 255.255.255.252
Router(config-if)# no sh
Router(config-if)# ex
```

**Gambar 4.2** *List* program pengalamatan *interface*

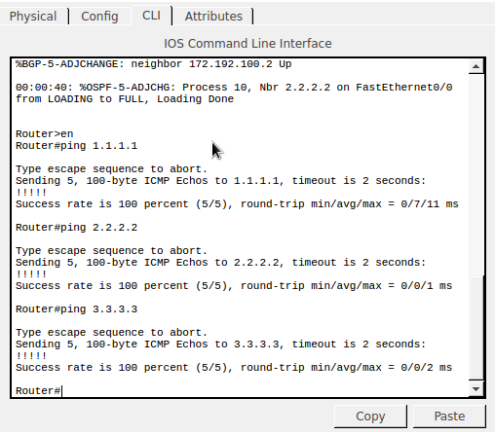
Pada gambar 4.3 ditunjukkan *list* program yang berisi konfigurasi *routing protocol* OSPF pada area 10. *List* program menunjukkan *network* berapa yang digunakan pada area 10. *Network* pada gambar 4.3 terdapat dua *network*, *network* pertama untuk *network* untuk *fastethernet* di area 10. Sedangkan untuk *network* kedua untuk *network loopback* di area 10. Di area 10 ada *router* 0, *router* 1, dan *router* 2. Jadi *list* program di bawah ini dimasukkan pada *router* di area 10.

```
Router> en
Router# conf t
Router(config)# router ospf 10
Router(config-router)# net 192.168.1.0 0.0.0.3 area 10
Router(config-router)# net 1.1.1.1 0.0.0.0 area 10
Router(config-router)# ex
```

**Gambar 4.3** *List* Program konfigurasi OSPF

Jika semua *router* di area 10 sudah diberikan *list* program seperti pada gambar 4.3, maka langkah selanjutnya adalah melakukan tes komunikasi *ping router*. Tes komunikasi *ping* kali ini dilakukan pada *router* langsung tanpa perlu dilakukan di komputer seperti pada umumnya. Program yang dituliskan yaitu *ping* 1.1.1.1, *ping* 2.2.2.2, dan *ping* 3.3.3.3. Ini menunjukkan apakah *router* 0 sampai *router* 2 sudah

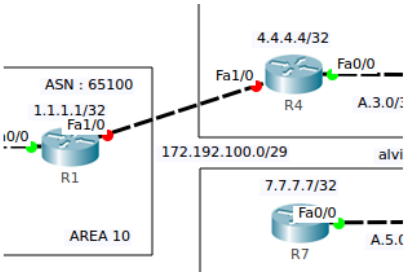
terkoneksi menggunakan *routing protocol* OSPF. Hasilnya dapat dilihat pada gambar 4.4 dengan menampilkan "*success rate is* 100 *percent*".




**Gambar 4.4** Tes Komunikasi *Ping Router* area 10

Untuk *router* di area 20 dan area 30 urutan *list* program yang dimasukkan sama seperti area 10. Jika sudah, maka jangan lupa untuk melakukan tes komunikasi *ping*. Setelah *router* area 10, area 20, dan area 30 sudah terhubung, langkah selanjutnya adalah melakukan konfigurasi alamat ip untuk menghubungkan *router* 0, *router* 3, dan *router* 6. *Routing protocol* yang digunakan yaitu *routing protocol* BGP. Pada *routing protocol* BGP terdapat nomer ASN di setiap area. ASN (*autonomous System Number*) merupakan nomor unik yang mengidentifikasi AS-AS. Untuk area 10 menggunakan ASN 65100. Di area 20 menggunakan ASN 65200. Dan pada area 30 menggunakan ASN 65300. Mengubungkan masing-masing area menggunakan kabel *cross*.

*Interface fastethernet1/0* digunakan untuk menghubungkan dari *router* 0 ke *router* 3. Alamat ip yang digunakan bisa dilihat di gambar 4.6. Jangan lupa memasukkan perintah "*no shutdown*" agar *port* tersebut selalu menyala. Terdapat perbedaan alamat ip antara *routing protocol* OSPF dengan *routing protocol* BGP. *Routing protocol* OSPF menggunakan alamat ip 192.168.x.x. Sedangkan *routing protocol* BGP menggunakan alamat ip 172.192.100.x. Hal ini bertujuan untuk membedakan antara *routing protocol* OSPF dengan BGP.



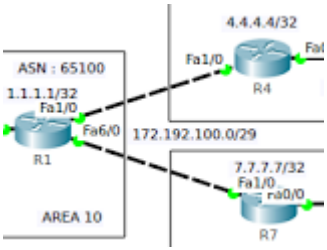

**Gambar 4.5** Konfigurasi *Routing protocol* BGP

```
Router> en
Router# conf t
Router(config)# int fa1/0
Router(config-if)# ip addr 172.192.100.1 255.255.255.248
Router(config-if)# no sh
Router(config-if)# ex
```

**Gambar 4.6** Konfigurasi Alamat IP untuk BGP

Semua *list* program untuk menghubungkan *router* 0, *router* 3, dan *router* 6 sudah dimasukkan maka semua *router* akan terhubung seperti pada gambar 4.7. Selanjutnya yaitu mengkonfigurasi *routing protocol* BGP di *router* 0, 3, dan 6.

*List* program yang digunakan untuk konfigurasi *routing protocol* BGP bisa dilihat pada gambar 4.8. Masukkan perintah "*router* bgp 65100" pada *router* 0. Hal ini menunjukkan bahwa *router* 0 diberikan nomer ASN 65100. *Redistribute* memiliki makna yaitu mendaftarkan *routing protocol* OSPF 10. Selanjutnya mengatur alamat ip tetangga dengan memasukkan alamat ip untuk *router* 3. Alamat ip ini digunakan untuk me-*remote router* tetangga yang memiliki ASN 65200. *Router* 0 ini didaftarkan sebagai bgp 65100 dengan *network* 192.168.1.1 untuk area 10 dan *network loopback*nya 1.1.1.1 untuk area 10. *List* program ini berlaku juga pada *router* 3 dan *router* 6.




**Gambar 4.7** Semua *Router* Sudah Terhubung

*List* program untuk *routing protocol* BGP sudah dimasukkan, maka selanjutnya yaitu tes komunikasi *ping* untuk *router* 0, *router* 3, dan *router* 6. Tes komunikasi *ping* sama seperti sebelumnya untuk *routing protocol* OSPF. Pada gambar 4.9 terlihat saat tes komunikasi *ping* ke ip 4.4.4.4, 7.7.7.7, dan 1.1.1.1 berjalan sukses. Hal ini dapat disimpulkan semua *router* sudah terhubung sehingga *test bed* jaringan IdREN sudah terbentuk.

```
Router> en
Router# conf t
Router(config)# router bgp 65100
Router(config-router)# redistribute ospf 10
Router(config-router)# neighbor 192.168.10.2 remote-as 65200
Router(config-router)# net 192.168.10.0 mask 255.255.255.0
Router(config-router)# ex
Router(config)# router ospf 10
Router(config-router)# redistribute bgp 65100 subnets tag 65100
Router(config-router)# net 10.10.10.0 0.0.0.255 area 0
Router(config-router)# net 1.1.1.1 0.0.0.0 area 0
Router(config-router)# ex
```

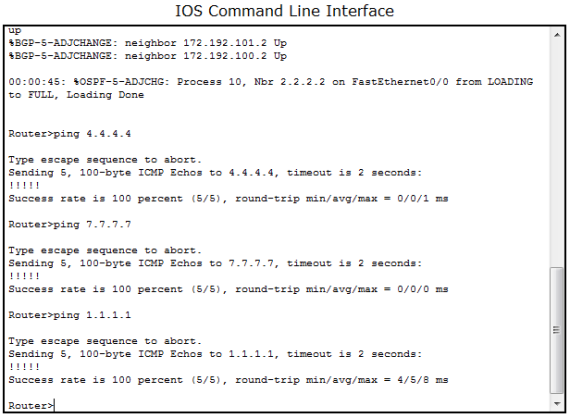
**Gambar 4.8** *List* Program *Routing protocol* BGP

## 4.2 Pembuatan *Identity Federation*

Berdasarkan perancangan sistem yang telah dibuat pada BAB 3, maka dihasilkan sebuah sistem autentikasi menggunakan LDAP dan RADIUS. Sistem ini menyediakan infrastruktur keamanan yang berdasarkan autentikasi data informasi akun pada direktori terpusat bertujuan untuk efisiensi pengelolaan jaringan antar perguruan tinggi. Pemanfaatan teknologi ini mengharuskan mahasiswa melakukan proses autentikasi terlebih dahulu sebelum menggunakan fasilitas internet, jika tidak maka penggunaan akses internet tidak bisa digunakan. Tahap pengujian pertama dalam sistem ini adalah melakukan pengujian

terhadap sistem autentikasi menggunakan LDAP dan RADIUS. Tahapan ini terbagi menjadi dua skenario pengujian yang dilakukan oleh admin, antara lain sebagai berikut :

1. Skenario pengujian *database* server LDAP dan antarmuka phpldapadmin
2. Skenario pengujian server RADIUS dan *captive portal*




**Gambar 4.9** Hasil Tes Komunikasi *Ping*

### 4.2.1 Perancangan *Database* Server LDAP

Tahap perancangan ini dilakukan untuk mengetahui bagaimana cara menggunakan dan mengelola sebuah *database* server LDAP menggunakan OpenLDAP yang berfungsi sebagai *backend database* yang digunakan untuk penyimpanan akun *login user*, selain itu ditambahkan juga antarmuka phpldapadmin yaitu perangkat lunak yang berbasis web yang berfungsi untuk mengatur dan memudahkan pengelolaan akun di dalam LDAP *database* server melalui web browser. Untuk memulai pengujian *database* server ini kita jalankan server yang sudah terinstal ubuntu server 16.04 dan openldap. Berikut adalah komputer server yang sudah terinstal ubuntu server 16.04 dan openldap yang ditunjukkan pada gambar 4.10


**Gambar 4.10** Perancangan Integrasi *Login* Sistem

Setelah openldap dijalankan pengelolaan *database* bisa diakses langsung melalui perangkat lunak berbasis web yaitu phpldapadmin yang bisa diakses melalui web browser dengan mengetikan alamat *url* ip *address* seperti berikut seperti berikut https://127.0.0.1/superldap ditunjukkan pada gambar 4.11


**Gambar 4.11** Tampilan Phpldapadmin

### 4.2.2 Perancangan Server RADIUS

Perancangan server RADIUS dilakukan dengan cara menguji hasil konfigurasi dan sinkronisasi terhadap *database* server LDAP untuk proses autentikasi *user* ketika *login*. Proses ini memungkinkan server RADIUS meneruskan paket data akun *user* yang diminta *user* dan melakukan sinkronisasi antara *database* server LDAP apakah data *user* yang di *request* terautentikasi atau tidak. Dalam pengujian ini server RADIUS menggunakan perangkat lunak FreeRADIUS yang bersifat *opensource* yang bisa digunakan sebagai RADIUS server. Untuk memulai pengujian telah disiapkan sebuah komputer yang sama dengan server LDAP yang sudah terinstal ubuntu server 16.04 dan freeRADIUS

server. Dalam server ini freeRADIUS telah selesai dikonfigurasi pada file modul LDAP untuk bisa binding ke server LDAP seperti pada gambar 4.12

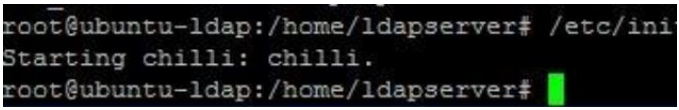

**Gambar 4.12** File Modul LDAP

File modul LDAP ini yang berfungsi untuk sinkronisasi dengan *database* server LDAP agar bisa saling terhubung ketika proses autentikasi berjalan. Dalam file modul LDAP ini diminta mengisi sertifikat server agar server RADIUS bisa mengakses *database* server LDAP untuk mengambil data dari *database* dengan perintah "server = "10.42.12.55"" yaitu IP *address database* server LDAP, domain component beserta password administrator *database* server LDAP "identity = "cn=admin,dc=test,dc=com"". Selanjutnya setelah semua proses konfigurasi selesai kita menjalankan debug program freeRADIUS agar bisa mengeksekusi file yang telah dimodifikasi. Terlebih dahulu harus menghentikan dengan perintah /etc/init.d/freeradius stop, setelah itu jalankan perintah freeRADIUS seperti yang ditunjukkan pada gambar 4.13


**Gambar 4.13** *Run* FreeRADIUS

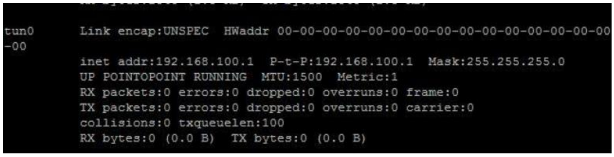
### 4.2.3 Perancangan *Captive Portal*

Perancangan *captive portal* ini dilakukan bersamaan dengan pengujian RADIUS dikarenakan komputer server yang dipakai untuk keduanya sama dalam satu server. Pengujian *captive port*al ini dilakukan dengan menguji proses autentikasi, tampilan antarmuka dan sistem yang dibangun agar semua interkoneksi jaringan dari *local* ke *public* berhasil diblok oleh *captive portal*. Selain itu pengujian ini mengharuskan *captive portal* bisa terhubung ke server RADIUS dalam mengambil data *user* di *database* server LDAP. Dalam pengujian ini perangkat lunak yang dipakai untuk membuat *captive portal* adalah coovachilli yang sudah terinstal pada komputer server yang memiliki sistem operasi ubuntu server 16.04 dan syarat komputer server ini harus memiliki 2 *ethernet* card. *Ethernet* 1 terhubung ke jaringan internet dan *ethernet* 2 terhubung ke jaringan *local*. Tahapan pertama dalam pengujian adalah dengan mulai menjalankan coovachilli dengan perintah /etc/init.d/chilli start seperti pada gambar 4.14




**Gambar 4.14** Menjalankan program Coovachilli

*Captive portal* mempunyai fungsi untuk memblok semua aliran paket data dan koneksi dari lokal ke publik dan mengharuskan *user* melakukan autentikasi terlebih dahulu apabila terhubung ke jaringan publik atau internet. Untuk itu ketika menjalankan coovachilli untuk bisa memakai fasilitas internet, coovachilli mempunyai fitur untuk membuat *tunel* secara otomatis dari *ethernet* yang terhubung ke jaringan lokal dalam kasus ini *ethernet* yang digunakan adalah eth1 dengan memberikan ip secara DHCP (*Dynamic Host Control Protocol*) dengan *range* ip dan *gateway* seperti pada gambar 4.15




**Gambar 4.15** *Tunnel Gateway*

Gambar 4.15 menunjukkan setelah coovachilli aktif akan menjalankan *tunneling* secara otomatis sesuai dengan konfigurasi yang dibuat. Dalam kasus ini *user* dari jaringan lokal akan diberi rentang ip dari 192.168.100.2 sampai dengan 192.168.100.254 secara DHCP sehingga *user* tidak perlu mengatur ip secara manual baik secara wireless maupun kabel.


**Gambar 4.16** Halaman *Login* Hotspot

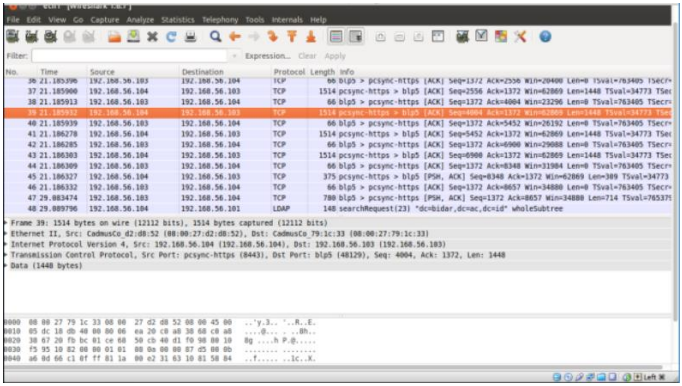
Pada gambar 4.16 menujukkan bahwa layanan *captive portal* telah berjalan karena terlebih dahulu *user* diarahkan ke *captive portal* untuk bisa mengkases jaringan. Pada gambar 4.16 Menunjukkan bahwa proses *login* berhasil dan *user* akan langsung medapatkan akses internet. Setelah *captive portal* berjalan, proses autentikasi akan diminta terus ketika *user* mengakses jaringan internet melalui web browser. Selama *user* belum melakukan proses autentikasi di halaman *login* ini, *user* tidak akan pernah bisa mengakses internet. Setiap kali *user* memasukkan alamat *url* apapun, halaman browser akan terus mendirect ke halaman *login* ini.


**Gambar 4.17** Halaman setelah *Login*

Jika proses autentikasi berhasil maka *user* sudah bisa mengakses jaringan internet, kemudian pada web *browser* akan menambahkan sesi halaman web baru untuk halaman *logout* seperti pada gambar 4.17 Tahap pengujian yang dilakukan menunjukkan sistem memiliki fungsi yang bekerja dengan benar.

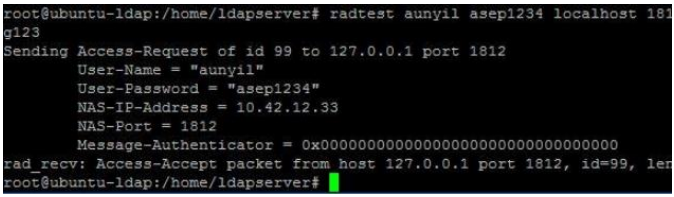
## 4.3 Pengujian Sistem

Pada pengujian untuk meninjau keamanan sistem dilakukan dengan mengcapture paket menggunakan tools *wireshark*. Pada saat login terlihat proses login dienkripsi menggunakan protokol https. Akan tetapi setelah proses login maka server LDAP akan mengirim respon query yang di dalamnya akan terlihat pengguna dan *domain* dari *quey* LDAP yang tidak dienkripsi menggunakan protokol LDAP 389. Tetapi hasilnya hanya berupa *success* atau *bindresponse* LDAP bukan password. Hal ini dapat dilihat di gambar 4. 18.



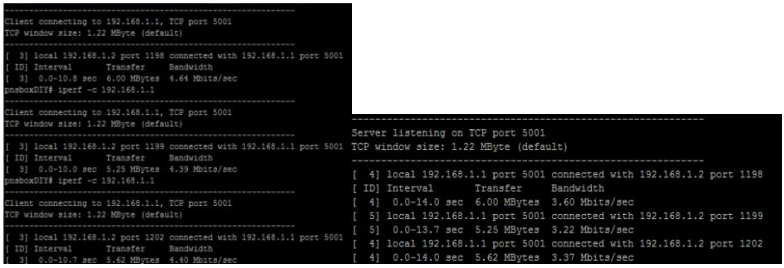
**Gambar 4.18** *Login* yang terenkripsi menggunakan HTTPS

Setelah menjalankan freeRADIUS langkah selanjutnya adalah mencoba melakukan *radtest* ke *database* server LDAP. *Radtest* adalah perintah yang dilakukan untuk mencoba mengambil data *user* oleh server radius untuk membuktikan proses binding ke server ldap telah tersambung. Yang dilakukan yaitu mencoba *radtest* ke akun *user* yang telah terdaftar di server ldap yaitu akun asep unyil. Perintah *radtest* bisa dilihat pada gambar 4.19




**Gambar 4.19** *Testing* RadTest

Pengujian *throughput* menggunakan *iperf* pada saat trafik kosong atau tidak ada data yang lewat maka hasilnya memiliki bandwidth 3Mbps. Hasil capture dapat dilihat di gambar 4.20. Pada gambar terlihat bahwa ada waktu pengiriman data, besar data yang dikirim serta besarnya *bandwidth*.




**Gambar 4.20** Hasil *capture throughput* dengan *bandwidth* 3Mbps

# BAB 5
# PENUTUP

Dari hasil yang telah didapatkan selama proses perancangan dan pengujian untuk tugas akhir ini, maka dapat diambil kesimpulan dan saran untuk dapat dilakukan perbaikan dan pengembangan sehingga bisa lebih bermanfaat.

## 5.1 Kesimpulan

Berdasarkan data hasil diperoleh beberapa kesimpulan antara lain sebagai berikut:

1. *Test bed* jaringan IdREN memakai dua jaringan. Jaringan utama yang menghubungkan *router* antar area kampus menggunakan *routing protocol* BGP. Sedangkan jaringan dibawahnya yang menghubungkan *router* di setiap area kampus menggunakan *routing protocol* OSPF. Pengujian test bed jaringan IdREN menggunakan iperf untuk mengetahui interval waktu, kapasitas data yang dikirim dan *bandwidth*.
2. *Sharing authority access* dirancang dengan konfigurasi RADIUS server sebagai autentikasi dan LDAP server sebagai *database*. RADIUS server terkoneksi dengan LDAP server menggunakan alamat ip LDAP server di *test bed* jaringan IdREN. Radtest digunakan untuk mengetahui koneksi RADIUS server dengan LDAP server.
3. *Security* dari tugas akhir ini menggunakan *protocol* HTTPS dalam komunikasi RADIUS server dengan *client*. RADIUS server menggunakan SSL dengan membangun *self signed certificate*. Pengujian keamanan menggunakan aplikasi *wireshark* untuk mengetahui bahwa proses autentikasi telah dienkripsi dengan protokol https.

## 5.2 Saran

Terkait dengan kendala dan kekurangan dalam penyusunan Tugas Akhir ini, ada beberapa hal yang dapat penulis sarankan untuk pengembangan selanjutnya. Antara lain sebagai berikut:

1. Masih banyak topik yang perlu dikembangkan di jaringan IdREN

2. Setelah membuat *Test bed* jaringan IdREN, diharapkan bisa diimplementasikan pada jaringan IdREN yang sebenarnya
3. Diharapkan tidak hanya bergantung pada satu perangkat saja, yaitu *cisco*. Masih banyak perangkat lain yang bisa mendukung topik ini.

# DAFTAR PUSTAKA


[1] Perez alejandro, Pereniguez Fernando, Marin Rafael, Lopez Gabriel and Howlett Josh – Identity Federations Beyond the Web: A Survey, IEEE Communication Surveys & Tutorials, Vol 16 no.4, Fourth Quarter 2014

[2] Vallado E. Tito, Bhawiyuga Adhitya, P. Eko Sakti – Analisis Perbandingan Unjuk Kerja Sistem Autentikasi Single Sign-On dengan Protokol LDAP dan RADIUS, Paper, April 2011

[3] Yuliansyah, H., Optimalisasi radius server sebagai system otentikasi dan otorisasi untuk proses login multi aplikasi web berbasis hph, Skripsi Universitas Ahmad Dahlan, Yogyakarta, 2011.

[4] Wijaya, B., Membangun Server AAA Menggunakan Protokol Remote Access Dial In User Service, Diploma Polteknik Negeri Jember, Jember, 2011

[5] Nurdeni Ade D, Suadi W., ―Implementasi Teknologi Single Sign On Di Lingkungan Teknik Informatika ITS, Tugas Akhir Institut Teknologi Sepuluh Nopember, Surabaya, 2011

[6] Bernal F., Sanchez M., Lopez G., Antonio F., Skarmeta-Gomez, Trusted Network Access Control in the eduroam federation, Third International Conference on Network and System Security, 2009

*Halaman ini sengaja dikosongkan*

# LAMPIRAN

Lembar Pengesahan Proposal Tugas Akhir

**Departemen Teknik Elektro**
Fakultas Teknologi Elektro – ITS

**TE 141599 TUGAS AKHIR – 4 SKS**

10 FEB 2017

| | | |
|---|---|---|
| Nama Mahasiswa | : | Ary Budi Prakoso |
| Nomer Pokok | : | 2215 105 060 |
| Bidang Studi | : | Telekomunikasi Multimedia |
| Tugas Diselesaikan | : | Semester Genap Th. 2016/2017 |
| Dosen Pembimbing | : | 1. Dr. Ir. Achmad Affandi, DEA<br>2. Ir. Djoko Suprajitno Rahardjo, MT. |
| Judul Tugas Akhir | : | **Pengembangan *Identity Federation* pada *Test Bed* IDREN (*Indonesian Research Education Network*) (*Developing Identity Federation at IDREN Test Bed*)** |

**Uraian Tugas Akhir** :
Pada bidang teknologi informasi, *Identity Federation* adalah sebuah kebijakan atau aturan untuk mengatur satu identitas antara pengguna dan perangkat pada jaringan yang berbeda. Jaringan IDREN adalah penghubung antar Pendidikan Tinggi dan Lembaga Riset di Indonesia. Satu akun dapat digunakan di berbagai kampus yang telah terhubung jaringan IDREN. Terdapat *sharing database* untuk mempermudah komunikasi antar Instansi. LDAP (*Light Weight Directory Access Protocol*) adalah sebuah protokol yang mendefinisikan bagaimana data disimpan secara terpusat dan dapat diakses melalui jaringan. Sebagai contoh, LDAP seringkali digunakan untuk menyimpan nama pengguna dan sandi yang terdapat di dalam sistem secara terpusat. Tugas Akhir ini bertujuan untuk membuat satu akun berisi nama pengguna dan sandi yang dapat digunakan pada test bed jaringan IDREN

Dosen Pembimbing I,

Dr. Ir. Achmad Affandi, DEA
NIP. 196510141990021001

Dosen Pembimbing II,

Ir. Djoko Suprajitno Rahardjo, MT.
NIP. 195506221987011000

Mengetahui,
Ketua Program Studi S1

Dedet C. Riawan, ST. M.Eng. Ph. D.
NIP. 197311192000031001

Menyetujui,
Kepala Laboratorium Jaringan Telekomunikasi B301

Dr. Ir. Achmad Affandi, DEA
NIP. 196510141990021001

Konfigurasi Interface

**Untuk Router 1**

```
Router> en
Router# conf t
Router(config)# int lo0
Router(config-if)# ip addr 1.1.1.1 255.255.255.255
Router(config-if)# ex
Router(config)# int fa0/0
Router(config-if)# ip addr 192.168.1.1 255.255.255.252
Router(config-if)# no sh
Router(config-if)# ex
```

---

**Untuk Router 2**

```
Router> en
Router# conf t
Router(config)# int lo0
Router(config-if)# ip addr 2.2.2.2 255.255.255.255
Router(config-if)# ex
Router(config)# int fa0/0
Router(config-if)# ip addr 192.168.1.2 255.255.255.252
Router(config-if)# no sh
Router(config-if)# ex
Router(config)# int fa1/0
Router(config-if)# ip addr 192.168.2.1 255.255.255.252
Router(config-if)# no sh
Router(config-if)# ex
```

**Untuk Router 3**

Router> **en**

Router# **conf t**

Router(config)# **int lo0**

Router(config-if)# **ip addr 3.3.3.3 255.255.255.255**

Router(config-if)# **ex**

Router(config)# **int fa1/0**

Router(config-if)# **ip addr 192.168.2.2 255.255.255.252**

Router(config-if)# **no sh**

Router(config-if)# **ex**

Konfigurasi routing protokol OSPF

**Untuk Router 1**

```
Router> en
Router# conf t
Router(config)# router ospf 10
Router(config-router)# net 192.168.1.0 0.0.0.3 area 10
Router(config-router)# net 1.1.1.1 0.0.0.0 area 10
Router(config-router)# ex
```

---

**Untuk Router 2**

```
Router> en
Router# conf t
Router(config)# router ospf 10
Router(config-router)# net 192.168.1.0 0.0.0.3 area 10
Router(config-router)#  net 192.168.2.0 0.0.0.3 area 10
Router(config-router)# net 2.2.2.2 0.0.0.0 area 10
Router(config-router)# ex
```

---

**Untuk Router3**

```
Router> en
Router# conf t
Router(config)# router ospf 10
Router(config-router)# net 192.168.2.0 0.0.0.3 area 10
Router(config-router)# net 3.3.3.3 0.0.0.0 area 10
Router(config-router)# ex
```

Konfigurasi interface

**Untuk Router1**

```
Router> en
Router# conf t
Router(config)# int fa1/0
Router(config-if)# ip addr 172.192.100.1 255.255.255.248
Router(config-if)# no sh
Router(config-if)# ex
```

---

**Untuk Router4**

```
Router> en
Router# conf t
Router(config)# int fa1/0
Router(config-if)# ip addr 172.192.100.2 255.255.255.248
Router(config-if)# no sh
Router(config-if)# ex
```

**Untuk Router1**

Router> **en**

Router# **conf t**

Router(config)# **int fa6/0**

Router(config-if)# **ip addr 172.192.101.1 255.255.255.248**

Router(config-if)# **no sh**

Router(config-if)# **ex**

---

**Untuk Router7**

Router> **en**

Router# **conf t**

Router(config)# **int fa1/0**

Router(config-if)# **ip addr 172.192.101.2 255.255.255.248**

Router(config-if)# **no sh**

Router(config-if)# **ex**

Konfigurasi routing protokol BGP

**Untuk Router 1**

```
Router> en
Router# conf t
Router(config)# router bgp 65100
Router(config-router)# redistribute ospf 10
Router(config-router)# neighbor 192.168.10.2 remote-as 65200
Router(config-router)# net 192.168.10.0 mask 255.255.255.0
Router(config-router)# ex
Router(config)# router ospf 10
Router(config-router)# redistribute bgp 65100 subnets tag 65100
Router(config-router)# net 10.10.10.0 0.0.0.255 area 0
Router(config-router)# net 1.1.1.1 0.0.0.0 area 0
Router(config-router)# ex
```

---

**Untuk Router 2**

```
Router> en
Router# conf t
Router(config)# router bgp 65200
Router(config-router)# redistribute ospf 10
Router(config-router)# neighbor 192.168.10.1 remote-as 65100
Router(config-router)# net 192.168.10.0 mask 255.255.255.0
Router(config-router)# ex
Router(config)# router ospf 10
Router(config-router)# redistribute bgp 65200 subnets tag 65200
Router(config-router)# net 10.10.11.0 0.0.0.255 area 0
Router(config-router)# net 2.2.2.2 0.0.0.0 area 0
Router(config-router)# ex
```

| Cisco 2800 Series Features | Cisco 2801 | Cisco 2811 | Cisco 2821 | Cisco 2851 |
|---|---|---|---|---|
| Target deployments | Data, voice, and video | Data, voice, and video | Data, enhanced voice, and video | Data, enhanced voice, and video |
| Default memory—Uses external compact Flash and on Cisco 2811, 2821, and 2851 Double Data Rate (DDR) error correction code (ECC) synchronous dynamic RAM (SDRAM) | Default/maximum<br>64-/128-MB compact Flash<br>128-/384-MB SDRAM | Default/maximum<br>64-/256-MB compact Flash<br>256-/768-MB DDR SDRAM with ECC | Default/maximum<br>64-/256-MB compact Flash<br>256-MB/1-GB DDR SDRAM with ECC | Default/maximum<br>64-/256-MB compact Flash<br>256-MB/1-GB DDR SDRAM with ECC |
| Fixed LAN ports with an RJ-45 port | 2 Fast Ethernet (10/100) | 2 Fast Ethernet (10/100) | 2 Gigabit Ethernet (10/100/1000) | 2 Gigabit Ethernet (10/100/1000) |
| Fixed USB ports (Version 1.1)—for future applications | 1 | 2 | 2 | 2 |

| Cisco 2800 Series Features | Cisco 2801 | Cisco 2811 | Cisco 2821 | Cisco 2851 |
|---|---|---|---|---|
| AIM slots (internal) | 2 | 2 | 2 | 2 |
| PVDM slots for optional PVDM2 | 2 | 2 | 3 | 3 |
| Onboard VPN encryption acceleration—IP Security (IPSec) DES, 3DES, AES128, AES192, and AES256 Note: requires Cisco IOS Software Security feature set | Yes | Yes | Yes | Yes |
| NME support—Cisco 2811, 2821, and 2851 can accommodate only one network-module slot or one NME slot. The NME has the same form factor as the network module, but offers higher-density applications compared to the current network module. A NME extended version (NME-X) also can be substituted in the Cisco 2821 or Cisco 2851, which is a wider form of the NME that will enable future services and functions. The Cisco 2851 also can substitute one double-wide high-density network module (NMD) or one NME-X double-wide version (NME-XD). | Not applicable<br>No network-module support on Cisco 2801 | NM<br>NME | NM<br>NME<br>NME-X | NM<br>NME<br>NME-X<br>NMD<br>NME-XD |
| EVM slots—The EVM offers additional voice services in a module format, using a single slot on the Cisco 2821 or Cisco 2851. Network-module or NME versions are not supported in this slot on the Cisco 2800 Series | 0 | 0 | 1 | 1 |
| Interface card slots—Each version can accommodate HWICs. These HWIC slots also support VICs, VWICs, and WICs. Alternatively, two side-by-side HWIC slots can be substituted to seat one double-wide HWIC (HWIC-D) | 4 slots total:<br>2 slots support HWIC, WIC, VIC, or VWIC type modules<br>1 slot supports WIC, VIC, or VWIC type modules<br>1 slot supports VIC or VWIC type modules | 4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules | 4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules | 4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules |

**Table 2.** Network Modules Not Supported by Cisco 2811, Cisco 2821, and Cisco 2851 routers

| | | |
|---|---|---|
| NM-1FE-FX | NM-2CE1U | NM-1A-OC3SMI-1V |
| NM-1FE-TX | NM-2CT1 | NM-1A-OC3SML-1V |
| NM-1FE-SMF | NM-2CT1-CSU | NM-1A-OC3-MM-EP |
| NM-1FEFX-V2(MMF) | NM-1A-OC3MM | NM-1A-OC3SMI-EP |
| NM-1FE1R2W | NM-1A-OC3SMI | NM-1A-OC3SML-EP |
| NM-1FE2W | NM-1A-OC3SML | NM-4T |
| NM-1FE2W-V2 | NM-1GE | NM-1V |
| NM-2FE2W | NM-1FE-MMF | NM-1CT1 |
| NM-2FE2W-V2 | NM-1FEFX-SMF | NM-8E1-IMA |
| NM-2W | NM-1CE1B | NM-8T1-IMA |
| NM-4E1-IMA | NM-1CE1U | NM-4T1-IMA |
| NM-1CT1-CSU | NM-2V | |
| NM-2CE1B | NM-1A-OC3MM-1V | |

**Table 3.** Unsupported WICs and Their Recommended Replacements for Cisco 2800 Series

| WICs Not Supported | Replacement WICs |
|---|---|
| WIC-4ESW | HWIC-4ESW or HWIC-D-9ESW |
| WIC-1B-S/T | WIC-1B-S/T-V3 |
| WIC-1B-U | WIC-1B-U-V2 |
| WIC-1B-S/T-LL | WIC-1B-S/T-V3 |
| WIC-1DSU-T1 | WIC-1DSU-T1-V2 |

**Table 4.** Interface Card Support on Cisco 2800 Series by Version

| Part Number | Cisco 2801 | Cisco 2811 | Cisco 2821 | Cisco 2851 |
|---|---|---|---|---|
| WIC-1SHDSL-V2 | No | Yes | Yes | Yes |
| HWIC-1GE-SFP | No | Yes | Yes | Yes |

# Switch Cisco 2960

**Table 1. Configurations of Cisco Catalyst 2960-S and 2960 Series Switches with LAN Lite Software**

| Switch Model | Description | Uplinks |
|---|---|---|
| Catalyst 2960-S Switches with 1 Gigabit Uplinks and 10/100/1000 Ethernet Connectivity | | |
| Cisco Catalyst 2960S-48TS-S | 48 Ethernet 10/100/1000 | 2 1 GbE ports |
| Cisco Catalyst 2960S-24TS-S | 24 Ethernet 10/100/1000 | 2 1 GbE SFP ports |
| Catalyst 2960 Switches with 1 Gigabit Uplinks and 10/100 Ethernet Connectivity | | |
| Cisco Catalyst 2960-48PST-S | 48 Ethernet 10/100 PoE ports (370W capacity) | 2 fixed 10/100/1000 ports and 2 SFP ports |
| Cisco Catalyst 2960-24PC-S | 24 Ethernet 10/100 PoE ports (370W capacity) | 2 dual-purpose ports (10/100/1000 or SFP) |
| Cisco Catalyst 2960-24LC-S | 24 Ethernet 10/100 and 8 10/100 PoE ports (123W capacity) | 2 dual-purpose ports (10/100/1000 or SFP) |
| Cisco Catalyst 2960-48TC-S | 48 Ethernet 10/100 | 2 dual-purpose ports (10/100/1000 or SFP) |
| Cisco Catalyst 2960-48TT-S | 48 Ethernet 10/100 | 2 fixed 10/100/1000 ports |
| Cisco Catalyst 2960-24TC-S | 24 Ethernet 10/100 | 2 dual-purpose ports (10/100/1000 or SFP) |
| Cisco Catalyst 2960-24-S | 24 Ethernet 10/100 | None |
| Compact Switches | | |
| Cisco Catalyst 2960-8TC-S | 8 Ethernet 10/100 compact size with no fan | 1 dual-purpose port (10/100/1000 or SFP) |

**Table 2. Switch PoE Power Capacity**

| Switch Model | Maximum Number of PoE Ports* | Available PoE Power |
|---|---|---|
| Cisco Catalyst 2960-48PST-S | 24 ports up to 15.4W<br>48 ports up to 7.7W | 370W |
| Cisco Catalyst 2960-24PC-S | 24 ports up to 15.4W | 370W |
| Cisco Catalyst 2960-24LC-S | 8 ports up to 15.4W | 123W |

**Table 3. Hardware Features for Cisco Catalyst 2960-S and 2960 Series Switches with LAN Lite Software**

| **Performance and Scalability Numbers for All Switch Models** | |
|---|---|
| Forwarding bandwidth | 16 Gbps (2960), 50 Gbps (2960-S) |
| Flash memory | 32 MB (2960), 64 MB (2960-S) |
| Memory DRAM | 64 MB (2960), 128 MB (2960-S) |
| Max VLANs | 64 |
| VLAN IDs | 4000 |
| Maximum transmission unit (MTU) | Up to 9198 bytes |
| Jumbo frames | 9016 bytes (2960), 9216 bytes (2960-S) |
| Forwarding Rate | |
| 2960S-48TS-S | 74.4 mpps |
| 2960S-24TS-S | 38.7 mpps |
| 2960-8TC-S | 2.7 mpps |
| 2960-24-S | 3.6 mpps |
| 2960-24TC-S | 6.5 mpps |
| 2960-24PC-S | 6.5 mpps |

| **Connectors and Cabling and Indicators** |
|---|
| • 10BASE-T ports: RJ-45 connectors, 2-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling<br>• 100BASE-TX ports: RJ-45 connectors, 2-pair Category 5 UTP cabling<br>• 1000BASE-T ports: RJ-45 connectors, 4-pair Category 5 UTP cabling<br>• 1000BASE-T SFP-based ports: RJ-45 connectors, 4-pair Category 5 UTP cabling<br>• 1000BASE-SX, -LX/LH SFP-based ports: LC fiber connectors (single- and multimode fiber)<br>• 100Base-FX: LC fiber connectors (single- and multimode fiber) |
| • Customers can provide power to a switch only by using the internal power supply. The connector is located at the back of the switch. These switches do not have a redundant-power-supply port.<br>• The internal power supply is an auto-ranging unit.<br>• The internal power supply supports input voltages between 100 and 240 VAC.<br>• Use the supplied AC power cord to connect the AC power connector to an AC power outlet. |
| • Per-port status: Link integrity, disabled, activity, speed, and full duplex<br>• System status: System, link status, link duplex, PoE, and link speed |
| • Per-port status: Link integrity, disabled, activity, speed, and full duplex<br>• System status: System, link status, link duplex, PoE, and link speed |

**Table 4. Power Specifications for Cisco Catalyst 2960-S and 2960 Series Switches with LAN Lite Software**

| Description | C2960-S and C2960 Specifications | | | | |
|---|---|---|---|---|---|
| Models | C2960S-48TS-S | C2960S-24TS-S | C2960-8TC-S | C2960-24TC-S | C2960-24PC-S |
| 100 Percent Throughput | | | | | |
| Measured Power Consumption | 53W | 36W | 12W | 22W | 27W |
| 5 Percent Throughput | | | | | |
| Measured Power Consumption | 50W | 36W | 11W | 21W | 24W |
| 5 Percent Throughput (with 50 Percent PoE Loads) | | | | | |
| Measured Power Consumption | - | - | - | - | Switch Power: 237W<br>PoE Power: 185W |
| 100 Percent Throughput (with Maximum Possible PoE Loads) | | | | | |
| Measured Power Consumption | - | - | - | - | Switch Power: 433W<br>PoE Power: 357W |

*Halaman ini sengaja dikosongkan*

# RIWAYAT PENULIS

**Ary Budi Prakoso.** dilahirkan di Surabaya, pada tanggal 21 Juni 1993. Merupakan putra kedua dari dua bersaudara pasangan Bapak Agus Rahardjo dan Ibu Sri Budiati. Penulis menamatkan sekolah di SDN Pucang I tahun 2005. Kemudian masuk ke SMPN 1 Sidoarjo, tamat tahun 2008. Melanjutkan di SMA Muhammadiyah 2 Sidoarjo pada tahun 2008. Tahun 2011, penulis melanjutkan pendidikan di D3 Teknik Elektro FTI (Fakultas Teknologi Industri), ITS (Institut Teknologi Sepuluh Nopember) Surabaya dan tamat pada tahun 2015. Selanjutnya penulis mengambil pendidikan S1 program Lintas Jalur di bidang dan tempat yang sama yaitu Jurusan Teknik Elektro, FTI - ITS Surabaya pada pertengahan tahun 2015. Penulis memilih bidang studi Telekomunikasi Multimedia dan mengambil topik Tugas Akhir di Laboratorium Jaringan Telekomunikasi.

E-mail :ary.ee.its@gmail.com

*Halaman ini sengaja dikosongkan*